

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN DRAGO,

Defendant.

No. 18 Cr. 394 (SJF)

**MEMORANDUM OF LAW IN SUPPORT OF
JOHN DRAGO'S MOTION TO SUPPRESS,
TO DISMISS THE INDICTMENT, AND FOR OTHER RELIEF**

Mintz, Levin, Cohn, Ferris,
Glovsky and Popeo, P.C.
666 Third Avenue
New York, NY 10017
(212) 659-7300
Attorneys for John Drago

TABLE OF CONTENTS

	Page
PRELIMINARY STATEMENT	1
STATEMENT OF FACTS	7
I. Background.....	7
A. John Drago's Personal, Educational, and Professional Background	7
B. Formation of Kayla Check Cashing Corp.....	8
C. Kayla's Reporting Requirements and Compliance Program	8
D. The Investigation and Search of Kayla.....	10
II. The Investigation.....	11
A. The Application and Supporting Affidavit to Search Kayla.....	11
1. The Affidavit's Justification for Supposed Probable Cause	11
2. Specifying Documents to Be Seized.....	15
B. The Kayla Warrant.....	17
C. The Execution of the Search of Kayla	18
D. After the August 2013 Search.....	19
E. The Indictment	20
F. The Application to Search John's Cell Phone	21
ARGUMENT	25
I. THE IRS KNOWINGLY EXECUTED A FACIALLY UNCONSTITUTIONAL SEARCH WARRANT IN AUGUST 2013, AND ITS FRUITS SHOULD BE SUPPRESSED.....	25
A. Constitutional Requirements for Search Warrants	25
B. The Kayla Warrant Fails to Describe with Particularity the Items To Be Seized.....	28
C. The Kayla Warrant Is Overbroad and Lacks Probable Cause	37
II. THE SNEDEKER AFFIDAVIT WAS MATERIALLY MISLEADING	43
A. Agent Snedeker's General Mischaracterization of Kayla.....	44
B. Agent Snedeker Omitted Recorded Information Tending to Exculpate the Boss (<i>i.e.</i> , John).....	47
C. Additional Omissions and Misleading Assertions.....	48
III. THE GOVERNMENT'S FIVE-YEAR RETENTION OF NEARLY EVERY FILE SEIZED CONSTITUTES AN UNREASONABLE SEARCH AND SEIZURE IN VIOLATION OF JOHN'S FOURTH AMENDMENT RIGHTS	51

IV. THE SEARCH AND SEIZURE OF JOHN'S CELL PHONE WERE UNCONSTITUTIONAL, AND ITS EVIDENCE MUST BE SUPPRESSED.....	54
A. The Government Unlawfully Seized John's Cell Phone	54
B. The Phone Warrant Is a Facially Invalid "General" Warrant	57
1. The Phone Warrant Does Not Describe with Particularity the Items to Be Seized	57
2. The List of Items is Overbroad and Lacks Probable Cause.....	61
3. The McCue Affidavit Was Materially Misleading	62
V. CERTAIN CHARGES SHOULD BE PARTICULARIZED OR DISMISSED	65
A. Count One Is Duplicitous.....	65
B. Count Two Should Be Dismissed Because John Is Not a "Financial Institution" or "Money Services Business"	67
C. The Government's Pre-Indictment Delay Requires Dismissal of the Indictment	68
VI. THE GOVERNMENT SHOULD PROVIDE A BILL OF PARTICULARS.....	72
A. The Ambiguity of the Indictment Warrants a Bill of Particulars.....	73
B. John's Request Is Narrowly Tailored to Seek Only that Information Necessary to Prepare His Defense and Avoid Unfair Surprise at Trial	80
VII. THE GOVERNMENT SHOULD BE ORDERED TO PRODUCE <i>BRADY</i> AND <i>GIGLIO</i> MATERIAL.....	82
CONCLUSION.....	83

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009).....	25, 54
<i>Brady v. Maryland</i> , 373 U.S. 83 (1963).....	1, 72, 82, 83
<i>Breitbart v. Mitchell</i> , 390 F. Supp. 2d 237 (E.D.N.Y. 2005)	57
<i>Bumper v. North Carolina</i> , 391 U.S. 543 (1968).....	56-57
<i>Chaplin v. Kirkpatrick</i> , No. 9:17-CV-0718(MAD/DEP), 2018 U.S. Dist. LEXIS 170975 (N.D.N.Y. Oct. 2, 2018)	69
<i>Chimel v. California</i> , 395 U.S. 752 (1969).....	55
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	26
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978).....	43, 50, 51, 64
<i>Frederique v. Cty. of Nassau</i> , 168 F. Supp. 3d 455 (E.D.N.Y. 2016)	25
<i>Giglio v. United States</i> , 405 U.S. 150 (1972).....	1, 72, 83, 83
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	29, 31, 34
<i>Herring v. United States</i> , 555 U.S. 135 (2009).....	27
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	55
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	26, 37, 57

<i>McDonald v. United States,</i> 335 U.S. 451 (1948).....	54
<i>Schurman v. Leonardo,</i> 768 F. Supp. 993 (S.D.N.Y. 1991)	71
<i>Symonds v. Griffin,</i> No. 15 CV 9423 (PGG) (KNF), 2018 U.S. Dist. LEXIS 105079 (S.D.N.Y. June 21, 2018).....	71-72
<i>United States v. Alston,</i> No. 15 Cr. 435 (CM), 2016 U.S. Dist. LEXIS 63776 (S.D.N.Y. Apr. 29, 2016).....	52
<i>United States v. Belkin,</i> No. 93-240, 1993 U.S. Dist. LEXIS 17202 (E.D. Pa. Dec. 8, 1993).....	78
<i>United States v. Bershchansky,</i> 788 F.3d 102 (2d Cir. 2015).....	27
<i>United States v. Bianco,</i> 998 F.2d 1112 (2d Cir. 1993).....	39, 33-34
<i>United States v. Bin Laden,</i> 92 F. Supp. 2d 225 (S.D.N.Y. 2000).....	74
<i>United States v. Bin Laden,</i> No. S(7) 98 Cr. 1023 (LBS), 2000 U.S. Dist. LEXIS 18957 (S.D.N.Y. Dec. 15, 2000)	27
<i>United States v. Bortnovsky,</i> 820 F.2d 572 (2d. Cir. 1987).....	73, 80
<i>United States v. Brown,</i> No. 10-CR-675 (SJF), 2011 U.S. Dist. LEXIS 81595 (E.D.N.Y. July 25, 2011)	82
<i>United States v. Buck,</i> 813 F.2d 588 (2d. Cir. 1987).....	26, 31, 34
<i>United States v. Butt,</i> No. 18-CR-00087 (NSR), 2018 U.S. Dist. LEXIS 169729 (S.D.N.Y. Oct. 1, 2018)	50, 64
<i>United States v. Calandra,</i> 414 U.S. 338 (1974).....	27
<i>United States v. Cioffi,</i> 668 F. Supp. 2d 385 (E.D.N.Y. 2009)	31, 35, 51

<i>United States v. Clark,</i> 638 F.3d 89 (2d Cir. 2011).....	31
<i>United States v. Cohan,</i> 628 F. Supp. 2d 355 (E.D.N.Y. 2009)	26, 42
<i>United States v. Comprehensive Drug Testing, Inc.,</i> 621 F.3d 1162 (9th Cir. 2010)	51, 52
<i>United States v. Conley,</i> No. 3:17-CR-214, 2018 U.S. Dist. LEXIS 160511 (D. Conn. Sept. 20, 2018)	38
<i>United States v. Coppa,</i> 267 F.3d 132 (2d Cir. 2001).....	82
<i>United States v. Cornielle,</i> 171 F.3d 748 (2d Cir. 1999).....	69
<i>United States v. Criminal Triumph Capital Grp., Inc.,</i> 211 F.R.D. 31 (D. Conn. 2002).....	37
<i>United States v. Crisci,</i> 273 F.3d 235 (2d Cir. 2001).....	66
<i>United States v. Debbi,</i> 244 F. Supp. 2d 235 (S.D.N.Y. 2003).....	52
<i>United States v. DeGroote,</i> 122 F.R.D. 131 (W.D.N.Y. 1988).....	78, 79, 80
<i>United States v. Deluca,</i> No. 11-CR-169A(F), 2013 U.S. Dist. LEXIS 145364 (W.D.N.Y. Oct. 7, 2013)	79
<i>United States v. DiMarco,</i> No. 12 CR 205 (RPP), 2013 U.S. Dist. LEXIS 16279 (S.D.N.Y. Feb. 5, 2013).....	54
<i>United States v. Dinero Express, Inc.,</i> No. 99 Cr. 975 (SWK), 2000 U.S. Dist. LEXIS 2439 (S.D.N.Y. Mar. 1, 2000).....	38
<i>United States v. DiScala,</i> No. 14-cr-399 (ENV), 2018 U.S. Dist. LEXIS 36817 (E.D.N.Y. Feb. 27, 2018)	29
<i>United States v. Elsberry,</i> 602 F.2d 1054 (2d Cir. 1979).....	69, 71
<i>United States v. Fleet Mgmt. Ltd.,</i> 521 F. Supp. 2d 436 (E.D. Pa. 2007)	36

<i>United States v. Galpin,</i> 720 F.3d 436 (2d Cir. 2013).....	<i>passim</i>
<i>United States v. Ganias,</i> 755 F.3d 125 (2d Cir. 2014).....	<i>passim</i>
<i>United States v. Ganias,</i> 824 F.3d 199 (2d Cir. 2016).....	35, 54, 58
<i>United States v. Gasperini,</i> No. 16-CR-441 (NGG), 2017 U.S. Dist. LEXIS 84116 (E.D.N.Y. May 31, 2017)	78
<i>United States v. George,</i> 975 F.2d 72 (2d Cir. 1992).....	29, 30, 31, 42
<i>United States v. Gigante,</i> 979 F. Supp. 959 (S.D.N.Y. 1997)	29, 34
<i>United States v. Gross,</i> 165 F. Supp. 2d 372 (E.D.N.Y. 2001)	69, 70, 72
<i>United States v. Gupta,</i> 848 F. Supp. 2d 491 (S.D.N.Y. 2012).....	83
<i>United States v. Hawit,</i> No. 15-cr-252 (PKC), 2017 U.S. Dist. LEXIS 23391 (E.D.N.Y. Feb. 17, 2017).....	77
<i>United States v. Hickey,</i> 16 F. Supp. 2d 223 (E.D.N.Y. 1998)	34
<i>United States v. Hill,</i> 459 F.3d 966 (9th Cir. 2006)	26
<i>United States v. Hillegas,</i> 578 F.2d 453 (2d Cir. 1978).....	68-69
<i>United States v. Hsia,</i> 24 F. Supp. 2d 14 (D.D.C. 1998).....	80-81
<i>United States v. Hunter,</i> 13 F. Supp. 2d 574 (D. Vt. 1998).....	36
<i>United States v. Jackson,</i> 488 F. Supp. 2d 866 (D. Neb. 2007).....	71
<i>United States v. Jacobson,</i> 4 F. Supp. 3d 515 (E.D.N.Y. 2014)	61

<i>United States v. Johns,</i> 851 F.2d 1131 (9th Cir. 1988)	50-51
<i>United States v. Kearney,</i> 451 F. Supp. 33 (S.D.N.Y. 1978)	67
<i>United States v. Kow,</i> 58 F.3d 423 (9th Cir. 1995)	31, 61
<i>United States v. Lartey,</i> 716 F.2d 955 (2d Cir. 1983).....	55
<i>United States v. Leary,</i> 846 F.2d 592 (10th Cir. 1988)	31, 32
<i>United States v. Leon,</i> No. 1:08-CR-65-1, 2008 U.S. Dist. LEXIS 93751 (D. Vt. Nov. 18, 2008).....	78
<i>United States v. Lovasco,</i> 431 U.S. 783 (1977).....	69, 72
<i>United States v. Luna,</i> No. 3:05cr58 (SRU), 2006 U.S. Dist. LEXIS 28947 (D. Conn. May 9, 2006)	77
<i>United States v. Lustyik,</i> 57 F. Supp. 3d 213 (S.D.N.Y. 2014).....	38
<i>United States v. Mahaffy,</i> 693 F.3d 113 (2d Cir. 2012).....	82-83
<i>United States v. Mandell,</i> 752 F.3d 544 (2d Cir. 2014).....	43
<i>United States v. Marion,</i> 404 U.S. 307 (1971).....	69-70
<i>United States v. Marotta,</i> 326 F. Supp. 377 (S.D.N.Y. 1971)	55, 56
<i>United States v. Maxwell,</i> 920 F.2d 1028 (D.C. Cir. 1990)	59
<i>United States v. Mazza-Alaluf,</i> 607 F.Supp. 2d 484 (S.D.N.Y. 2009).....	48
<i>United States v. McMurtrey,</i> 704 F.3d 502 (7th Cir. 2013)	50

<i>United States v. Metter,</i> 860 F. Supp. 2d 205 (E.D.N.Y. 2012)	52, 53
<i>United States v. Morisse,</i> 660 F.2d 132 (5th Cir. 1981)	58-59
<i>United States v. Morris,</i> No. CR 07-2009 (NG) (JO), 2007 U.S. Dist. LEXIS 104248 (E.D.N.Y. Oct. 31, 2007)	27
<i>United States v. Morrison,</i> 518 F. Supp. 917 (S.D.N.Y. 1981)	71
<i>United States v. Murray,</i> 618 F.2d 892 (2d Cir. 1980).....	66
<i>United States v. Nekritin,</i> No. 10-cr-491 (S-1) (KAM), 2011 U.S. Dist. LEXIS 47407 (E.D.N.Y. May 3, 2011)	73-74
<i>United States v. O'Connor,</i> 237 F.2d 466 (2d Cir. 1956).....	78
<i>United States v. Onassis,</i> 125 F. Supp. 190 (D.D.C. 1954).....	77
<i>United States v. Otero,</i> 563 F.3d 1127 (10th Cir. 2009)	36
<i>United States v. Paulino,</i> 445 F.3d 211 (2d Cir. 2006).....	82
<i>United States v. Pirro,</i> 212 F.3d 86 (2d Cir. 2000).....	67
<i>United States v. Rajaratnam,</i> No. 09 Cr. 1184 (RJH), 2010 U.S. Dist. LEXIS 70385 (S.D.N.Y. July 13, 2010)	64, 74
<i>United States v. Raue,</i> No. CR. 07-30100-02, 2008 U.S. Dist. LEXIS 91827 (D.S.D. Nov. 12, 2008)	77-78
<i>United States v. Riley,</i> 906 F.2d 841 (2d Cir. 1990).....	28
<i>United States v. Roche,</i> 614 F.2d 6 (1st Cir. 1980).....	32, 59

<i>United States v. Rodriguez,</i> 496 F.3d 221 (2d Cir. 2007).....	82
<i>United States v. Rollack,</i> 90 F. Supp. 2d 263 (S.D.N.Y. 1999).....	31
<i>United States v. Rosa,</i> 626 F.3d 56 (2d Cir. 2010).....	30, 41, 58
<i>United States v. Santiago,</i> 987 F. Supp. 2d 465 (S.D.N.Y. 2013).....	69, 70, 71
<i>United States v. Savin,</i> No. 00 Cr. 45 (RWS), 2001 U.S. Dist. LEXIS 2445 (S.D.N.Y. Mar. 7, 2001).....	76, 80
<i>United States v. Scully,</i> 108 F. Supp. 3d 59 (E.D.N.Y. 2015)	38, 43, 73, 79
<i>United States v. SDI Future Health, Inc.,</i> 568 F.3d 684 (9th Cir. 2009)	33
<i>United States v. Shi Yan Liu,</i> 239 F.3d 138 (2d Cir. 2000).....	28-29
<i>United States v. Soliman,</i> No. 06-CR-236, 2008 U.S. Dist. LEXIS 87304 (W.D.N.Y. Oct. 29, 2008).....	52
<i>United States v. Spur Knitting Mills, Inc.,</i> 187 F. Supp. 653 (S.D.N.Y. 1960)	77
<i>United States v. Stern,</i> No. 03 Cr. 81 (MBM), 2003 U.S. Dist. LEXIS 20936 (S.D.N.Y. Nov. 19, 2003)	74
<i>United States v. Sturdivant,</i> 244 F.3d 71 (2d. Cir. 2001).....	65
<i>United States v. Tamura,</i> 694 F.2d 591 (9th Cir. 1982)	52-53
<i>United States v. Taylor,</i> 17 F. Supp. 3d 162 (E.D.N.Y. 2014)	82
<i>United States v. Trie,</i> 21 F. Supp. 2d 7 (D.D.C. 1998).....	76, 79, 81
<i>United States v. Triumph Capital Grp., Inc.,</i> 544 F.3d 149 (2d Cir. 2008).....	83

<i>United States v. Ulbricht,</i> 858 F.3d 71 (2d Cir. 2017).....	51
<i>United States v. Vilar,</i> No. S3 05-CR-621 (KMK), 2007 U.S. Dist. LEXIS 26993 (S.D.N.Y. Apr. 4. 2007)	29, 30, 31, 59
<i>United States v. Voustianiouk,</i> 685 F.3d 206 (2d Cir. 2012).....	28
<i>United States v. Wai Ho Tsang,</i> 632 F. Supp. 1336 (S.D.N.Y. 1986).....	72
<i>United States v. Walters,</i> 963 F. Supp. 2d 125 (E.D.N.Y. 2013)	78
<i>United States v. Westover,</i> 812 F. Supp. 38 (D. Vt. 1992).....	50
<i>United States v. Wey,</i> 256 F.Supp. 3d 355 (S.D.N.Y. 2017).....	<i>passim</i>
<i>United States v. Willis,</i> 475 F. Supp. 2d 269 (W.D.N.Y. 2007)	67
<i>United States v. Wilson,</i> No. 95 Cr. 668 (LMM), 1997 U.S. Dist. LEXIS 125 (S.D.N.Y. Jan. 8, 1997)	67
<i>United States v. Young,</i> 745 F.2d 733 (2d Cir. 1984).....	28
<i>United States v. Zemlyansky,</i> 945 F. Supp. 2d 438 (S.D.N.Y. 2013).....	<i>passim</i>
<i>United States v. Zhong,</i> No. 16-cr-614 (DLI), 2017 U.S. Dist. LEXIS 175357 (E.D.N.Y. Oct. 23, 2017)	73
<i>Walczak v. Rio,</i> 496 F.3d 139 (2d Cir. 2007).....	38
Statutes and Rules	
3 N.Y.C.R.R. § 400.14.....	12, 45
18 U.S.C. § 371.....	22, 23, 59
18 U.S.C. § 666.....	22, 59

18 U.S.C. § 1341.....	22, 32, 59
18 U.S.C. § 1343.....	22, 23, 59
18 U.S.C. § 1349.....	22, 23, 59
18 U.S.C. § 1956.....	22, 23, 59
18 U.S.C. § 1957.....	22, 23, 59
31 C.F.R. 1022.210.....	67, 68
31 C.F.R. 1010.100(ff).....	49
31 C.F.R. 1022.320(1)	49
31 U.S.C. § 5311.....	32
31 U.S.C. § 5318.....	67, 68
31 U.S.C. § 5322.....	66
31 U.S.C. § 5324.....	11
31 U.S.C. § 5332.....	32
Fed. R. Crim. P. 7(f)	73
Fed. R. Crim. P. 8(a)	65
Fed. R. Crim. P. 49.1	13
U.S. Const. amend. IV	<i>passim</i>
U.S. Const. amend. V.....	69
U.S. Const. amend. VI.....	73
Other Authorities	
2 Wayne R. LaFave, <i>Search and Seizure: A Treatise on the Fourth Amendment</i> § 4.6(a) (5 ed. 2012).....	38
Arjun Kharpal, <i>Samsung launches the Galaxy S9 smartphone to take on Apple's iPhone X</i> , CNBC (Feb. 25, 2018 1:58 PM), https://www.cnbc.com/2018/02/25/samsung-galaxy-s9-launches-at-mobile-world-congress-specs-price.html	24

Exec. Office for U.S. Attorneys, <i>Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations</i> , 77 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf	52
<i>MSBs Subject the SAR Requirement</i> , FinCEN, https://www.fincen.gov/msbs-subject-sar-requirement (last visited Nov. 30, 2018).....	15, 49

John Drago, by his attorneys, Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo, P.C., submits this memorandum of law in support of his pretrial motions to: (a) suppress evidence seized pursuant to a search warrant executed by the Internal Revenue Service (“IRS”) on or about August 6, 2013 at his company’s office; (b) suppress evidence obtained from his cell phone, which was seized at the time of his arrest, on or about August 1, 2018; (c) dismiss the Indictment (or certain Counts) on various grounds including for duplicity, failure to state an offense, and for pre-indictment delay; and (d) obtain from the Government a bill of particulars and *Brady* and *Giglio* materials.¹

PRELIMINARY STATEMENT

On August 6, 2013, the IRS violated John Drago’s Fourth Amendment rights when they entered his check-cashing business and executed a patently defective “general warrant” that granted the Government blanket authority to search for evidence of unspecified criminal activity. After executing that unconstitutional search, the Government brought no charges against the business or John – for the next *five years*. John’s rights were further violated because the IRS sat on the entire cache of improperly seized material, never purging or returning anything.

Then, only days before the fifth anniversary of that search, on August 1, 2018, the IRS arrested John. The charges against him appear to be based on facts entirely known to the IRS on or about the date of that 2013 search – alleging misconduct between 2010 and 2013. Upon John’s 2018 arrest, agents seized his cell phone – a phone that *did not even exist in 2013* – and then violated John’s constitutional rights again by misleading the Magistrate Judge into issuing a search warrant for that cell phone premised on alleged conduct from 2013 and earlier. The fruits

¹ *Brady v. Maryland*, 373 U.S. 83 (1963); *Giglio v. United States*, 405 U.S. 150 (1972).

of both searches should be suppressed because they plainly violated John’s Fourth Amendment rights.

The Indictment itself fails, too, for various reasons. For example, it charges that John failed to file one or more unspecified currency transaction reports (“CTRs”) and “structured” unspecified transactions to avoid filing CTRs at some unspecified date(s) and time(s) during an almost four-year span, despite the fact that his business filed more than *eight thousand* such reports in those years. It also charged John with failing to maintain an effective Anti-Money Laundering (“AML”) program over (or at some point during) a three-year span, despite the IRS’s own audits concluding his program was appropriate. None of the charges describe, with any detail at all, what actions by John violated the law. John moves to dismiss the Indictment because, among other things, the charges fail to apprise him adequately of his alleged crimes, and because they were brought after an unjustifiable and unexplained delay. Absent dismissal, John moves for a bill of particulars, and other related relief.

* * *

The 2013 warrant violated the Fourth Amendment’s “Particularity” clause because, on its face, it contained no meaningful limitations on what the agents could seize. Critically, the warrant failed to specify what crimes the government agents were investigating. The warrant did not substantively describe any wrongdoing, nor was any criminal code section even referenced to suggest the subject of the Government’s inquiry. The facial defects of the warrant were so plain that no law enforcement agent could reasonably have relied on it.

This is not merely some technical issue raised only with the benefit of hindsight. Indeed, John raised the patent defects in the warrant directly to the agents as soon as he saw it on August 6, 2013. The agents then examined the warrant and realized that it was defective (and admitted

as much to John), but instead of stopping the search and obtaining a valid warrant, the agents pushed ahead with their search knowing it was based on a defective warrant.

Beyond that fatal flaw, there are others as well. The warrant also listed 10 broad categories, including catch-all phrases that expanded those categories immeasurably, to justify the seizure of virtually every conceivable record that could exist at a check-cashing company. This included sweeping instructions to seize materials that “reflect financial transactions,” materials that “[regard] the identity of customers,” and materials “[regarding] the identity of Kayla’s employees.” Moreover, the categories listed every conceivable type of object that could contain information. As a result, the warrant provided the agents with no true guidance whatsoever on what should (and should not) be seized. Unsurprisingly, under these conditions, the agents seized virtually everything, including images of the entire hard drives from 11 computers, and more than 25 boxes of hard copy materials.

After the unconstitutional 2013 search of the Kayla office, as the days and years passed by, little clarity emerged. While the Government provided John with an electronic copy of the data from the hard drives that they seized in 2016, no documents were ever returned, and John was never informed what, if any, of the material taken – including the electronic copies that the Government retained – was deemed non-responsive to the warrants, or purged as such. The Government simply kept it all.

Almost exactly five years later, on August 1, 2018, John was awoken at about 7:00 am at his home, handcuffed in front of his wife, Victoria, and his 11-year-old daughter, and taken into custody (despite the fact that the Government must have believed he was not a flight risk, since they did not lodge charges against him for five years after executing the search warrant). Before leaving the house, the IRS agents escorted John to his bedroom upstairs, handed him a cellular

phone, and thereafter seized that phone. One agent originally stated that he had the right to seize his phone because it was “on” him when he was arrested, while another agent stated that they had a warrant for it. In reality, no search warrant authorizing the seizure of John’s phone existed at that time. A warrant obtained *hours later*, which the Government now posits authorizes a review of John’s seized phone – is also invalid on its face for several reasons (among others, it too is a general warrant), and was based on no probable cause at all.

The Indictment charges John with eight felony counts, including violations of the Bank Secrecy Act for failing to file “one or more” CTRs, failing to maintain an effective AML program, and structuring “one or more” financial transactions; and for violations of the Internal Revenue laws for failure to collect and pay Federal Insurance Contributions Act (FICA) tax.

Shortly after the Indictment, the Government produced the written application the IRS submitted to obtain the search warrant in August 2013. While some of the Indictment’s theories appear to echo those described in the 2013 warrant application, given the Indictment’s alarming lack of clarity, it is not clear how, when, and what John is alleged to have done to violate the law. What is clear, however, is that the Government’s presentation in 2013 to the Magistrate Judge was incomplete and misleading in several material respects. For example, the application failed to make clear that several of the undercover recordings made by the IRS tended to *exculpate* John: recorded conversations show salespeople explicitly describing “the boss” as someone who, e.g., likes them “to do things the right way.” Further, the 2013 warrant application repeatedly mischaracterized the business of check-cashing as inherently nefarious, in part by suggesting that Kayla’s customers are willing to pay a fee to Kayla that would not be charged by a traditional bank. In fact, corporate customers regularly and willingly pay this *perfectly legal* fee for the wholly legitimate purpose of obtaining funds from Kayla immediately to pay workers or

subcontractors, when traditional banks require a waiting period, often of several days. The 2013 warrant application also touted misleading statistics to suggest that large portions of the check-cashing traffic at John’s business went unreported when, in fact, the vast majority of check-cashing activity through the business would never have required the filing of reports. These facts, along with others, raise significant doubts as to whether the Magistrate Judge would have signed the warrant had he known the full story.

In short, this was not a reasonable effort to conduct a targeted investigation into specific wrongdoing. This was a fishing expedition into the workings of John’s business – a business that, right up to when John was arrested, was still getting exemplary marks on audits evaluating its compliance with Bank Secrecy Act (“BSA”) requirements.

Further, the 10-page Indictment woefully fails to apprise John of the charges against him. He is charged with failing to file “one or more” CTRs during the period between January 1, 2010 and October 31, 2013 – almost a *four-year* span – but the Indictment does not identify a single transaction during that span for which a CTR should have been filed but was not. This is despite the fact that John’s business processed hundreds of thousands of transactions during those years. Similarly, he is also charged with “structuring” cash transactions to avoid filing CTRs over that same time frame, but the Indictment includes no specifics about when such structuring occurred, or for which customers, or on which days. For the several FICA tax-related offenses, the Indictment fails to identify the employees for whom tax was not withheld, the amounts, or the time frames at issue. In other words, the defense has been left to guess what and how many wrong(s) he is charged with, saddling him with the task of locating “one or more” needles in a virtual field of haystacks to predict which of the hundreds of thousands of transactions performed by Kayla in the relevant period might be at issue.

The ambiguity of the Indictment violates John’s constitutional rights to have clear notice of and to understand the charges against him. Count One is fatally duplicitous because it charges John with failing to file “one or more” reports as a part of a “pattern,” which necessarily involves a jury determination on whether *multiple* reports were (or were not) filed. As written, the ambiguity of Count One makes it impossible to determine if jurors would be unanimous as to any one particular alleged reporting failure. Count Three, which charges John with structuring, may also be duplicitous for the same reason, but there simply is not enough information in the Indictment to ascertain whether he is charged with multiple instances of structuring or for multiple customers (or both). Count Two improperly charges John – an individual – with a violation of a statute that requires “financial institutions” and “money services businesses” to maintain an effective AML program. More generally, because the Government inexplicably waited five years to indict John, the entire Indictment should be dismissed on the grounds of unwarranted pre-indictment delay. If not dismissed in its entirety, this Indictment is a textbook example of when the Government should be ordered to provide a bill of particulars.

Finally, the instant Indictment – charging activity ending no later than October 2013 – purportedly provided the basis for another violation of John’s Fourth Amendment rights, at the time of his 2018 arrest: the unconstitutional seizure and search of his cell phone. Beyond the fact of the cell phone’s unjustified seizure, the warrant obtained for it after its seizure, authorizing agents to review the phone’s contents, also violates the Fourth Amendment’s Particularity Clause (among other facial problems). The Government admits in its warrant application that it planned to review the entirety of its contents to gauge whether any of the text messages, emails, call logs, and photos (among other things) on it are “evidence” of one of several crimes – including *several crimes not charged in the Indictment*. This is despite the fact

that the cell phone in question was not even in existence at the time of the indicted criminal activity. Thus, for the reasons set forth below, any fruits of the seizure of the cell phone should thus be suppressed as well.

STATEMENT OF FACTS

I. Background

A. John Drago's Personal, Educational, and Professional Background

John Drago was born in New York on July 12, 1964, the son of a homemaker and computer repair technician. He attended Johns Hopkins University on a full Army Reserve Officers' Training Corps ("ROTC") scholarship, and graduated in 1986 with a bachelors' degree in biology. With extraordinary pride for his country, John enlisted in the United States Military in 1983, where he rose in the ranks and eventually served during the Gulf War in 1990 and 1991 as a First Lieutenant. John currently lives on Long Island, New York, with his wife, Victoria Drago, and daughter.

John has spent more than 30 years in the check-cashing industry, where he began as a cashier under his then father-in-law, Frank Fede, the founder of Kayla Check Cashing Corp.'s predecessor, Mid Island Check Cashing Corp. During that time, the business grew from one to eight storefronts in Long Island, serving more than 10,000 customers each year, and processing approximately \$150 million in transactions each year. The businesses employ approximately 25 people, including cashiers, bookkeepers, sales people, and a compliance officer. Over the years, John has handled virtually every role in the business, ranging from cashier to compliance officer. John credits Kayla's success to his sense of discipline and desire to keep his affairs in order, something he learned in the military and has tried to continue ever since.

B. Formation of Kayla Check Cashing Corp.

Kayla and its predecessor, Mid Island Check Cashing Corp., have been licensed check cashers since 1976, when they were founded by John's former father-in-law, Frank Fede. In or around 1992, after John returned home from the Gulf War, he and his then wife, Lisa Lentini, opened three of their own stores, South Island Check Cashing Corp. ("South Island"), East Island Check Cashing Corp. ("East Island"), and North Island Check Cashing Corp. ("North Island"). With success in these stores, Ms. Lentini and John opened four more stores between 1994 and 1998 – two storefronts, located in Brentwood, and Uniondale, Long Island, which operated as Brentwood Check Cashing Corp. ("Brentwood"), another storefront, located in Elmont, Long Island, which operated with the already-existing location of North Island, and Bayshore Check Cashing Corp. ("Bayshore"). In 1997, Ms. Lentini and John purchased Mid Island Check Cashing Corp. and renamed it "Kayla Check Cashing Corp." (with South Island, East Island, Brentwood, North Island, and Bayshore, "Kayla"). About nine years later, in 2006, they opened up a company called Hogwarts, Inc., which serves as the management company for Kayla. What started as one store and a small, family-run operation, has grown into a six-store business, duly licensed by the New York State Department of Financial Services to serve as a check casher servicing the Suffolk County, Long Island Community.

During this time, John became active in managing and operating Kayla, and served as Vice President until his very recent resignation in October 2018. He also served as Kayla's compliance officer until the beginning of 2016. Until October 2018, John oversaw the day-to-day operations of Kayla.

C. Kayla's Reporting Requirements and Compliance Program

Kayla provides vital services to thousands of individuals and corporate customers for a small percentage fee of a given transaction. Many of Kayla's customers are individuals who do

not have bank accounts, perhaps because they have poor credit or because they lack sufficient funds to maintain a checking account, but who require the ability to cash checks and/or pay household bills. Similarly, Kayla's corporate customers, including contractors, use its services because Kayla is willing and able to provide funds immediately without requiring the customers to wait anywhere from one to ten business days (as depository banks often do) for access to those funds.

In accordance with longstanding legal requirements, if any customer (whether an individual or corporate) receives cash that totals \$10,000 or more (in the aggregate) in one business day, Kayla is obligated to file a currency transaction report, or CTR, with the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN"). These reports provide a financial paper trail, which assists FinCEN and other enforcement agencies in, among other things, monitoring certain entities and individuals for possible money laundering activity. Kayla filed thousands of CTRs per year, amounting to, during the relevant time frame, a total exceeding 8,000 such reports. Although not required to do so, Kayla voluntarily filed suspicious activity reports ("SARs") when it suspected that a customer was engaged in irregular, unexplained, or suspicious monetary transaction activity. SARs are a very helpful tool for law enforcement.

Kayla's internal processes for complying with its regulatory reporting requirements are outlined in its written AML program, which was put in place in accordance with the requirements of the BSA. In addition to a framework for reporting transactions, Kayla's AML program covers the following, among other things: policies and procedures for reporting transactions; designation of a compliance officer tasked with overseeing and monitoring Kayla's compliance with the BSA and other reporting requirements, and setting forth that officer's duties

and responsibilities; a regular and ongoing employee training program, including mandatory instruction on AML policies twice a year; and provision for audits of the compliance program by qualified outside auditors. *See Drago Aff. ¶ 2; Ex. 1; see also Siegal Aff., Ex. 1 (July 29, 2013 Affidavit of Special Agent Michael Snedeker (hereinafter, the “Snedeker Affidavit”) at ¶ 28 (“BSA compliance reviews of Kayla by the IRS for years 2007 and 2008 documented Kayla’s AML program. Their program includes regular and ongoing training for the employees of Kayla on current BSA laws, changes in regulations, and the employees’ responsibilities as they relate to said laws. Once completed, the training is acknowledged with the employees[’] signature. Kayla maintains records of its employees[’] training.”).*

Kayla’s AML program is audited regularly by Kayla’s appointed independent auditor, who, earlier in his career, was an auditor for the IRS. Drago Aff. ¶ 2. In addition, the New York State Department of Financial Services (“DFS”) also conducts an annual review of Kayla. *Id.* ¶ 3. Kayla’s depository bank (BNB Bank) has conducted regular reviews of the Kayla operation too. Kayla has routinely passed these independent, regular audits with high marks, both during and after the period covered by the Indictment, and in fact, has been praised by the IRS recently to “continue your high level of compliance with BSA regulations.” *See id.* ¶ 3, Ex. 2.

D. The Investigation and Search of Kayla

IRS Special Agent Michael Snedeker began an investigation of Kayla no later than February 2012, presumably as a part of “Operation Chokepoint,” the joint initiative between the IRS and the United States Department of Justice to “crack down” on the customers of commercial check-cashing companies.² About a year-and-a-half later, on August 6, 2013, the

² In August 2017, the United States Department of Justice stated that “law abiding businesses should not be targeted simply for operating in an industry that a particular administration might disfavor” and confirmed that “[a]ll of the Department’s bank investigations conducted as a part of Operation Chokepoint are now over.” *See Letter from*

IRS searched Kayla's offices pursuant to the search warrant (the "Kayla Warrant") that is the subject of this motion. No charges were filed at that time, nor in the nearly five years that followed, against either John Drago or Kayla.

II. The Investigation

A. The Application and Supporting Affidavit to Search Kayla

On July 29, 2013, the Government applied for a warrant to search the premises located at 1911 Broadhollow Road, Farmingdale, New York, which the warrant described as Kayla Check Cashing Corp. (the "Kayla Warrant"). Siegal Aff., Ex. 2. The supporting affidavit was sworn by IRS Special Agent Michael Snedeker. *Id.*, Ex. 1. The warrant application sought authorization to search for and seize evidence of violations of the BSA, specifically 31 U.S.C. § 5324. *Id.*

1. The Affidavit's Justification for Supposed Probable Cause

The Snedeker Affidavit broadly asserted that there was probable cause to believe that evidence of structuring in violation of the BSA would be found at Kayla. Agent Snedeker alleged that Kayla is known in the construction industry for assisting customers in evading income and payroll taxes.³ *Id.*, Ex. 1 at ¶¶ 12, 18, 22. To establish probable cause, the Snedeker Affidavit relied on, among other things, mischaracterizations of lawful check-cashing activity, recordings of purported bad actions primarily by two salepeople, skewed statistical analyses, and the fact that certain unaffiliated individuals or businesses who at some point were customers of Kayla's services had committed tax crimes of their own.

To justify the issuance of the Kayla Warrant, the Snedeker Affidavit painted a fundamentally skewed and unfair picture of the business of check-cashing. Through omissions

Stephen E. Boyd, Assistant Attorney General, to the Hon. Bob Goodlatte, Chairman of the Committee on the Judiciary, available at https://judiciary.house.gov/wp-content/uploads/2017/08/081617_Operation-Chokepoint.pdf.

³ Agent Snedeker further asserted, based on rank hearsay from one unnamed witness, that Kayla is "known within the construction industry" for "routinely assisting customers to evade income and payroll taxes." *Id.*, Ex. 1 at ¶ 12.

and misleading assertions, Agent Snedeker suggested that most, if not all, of the check-cashing industry is illegal. For instance, Agent Snedeker began by suggesting that customers use check-cashing companies like Kayla rather than traditional banks to evade reporting requirements, even if it means paying a two to three percent fee on each of the transactions. *Id.*, Ex. 1 at ¶ 9.

Agent Snedeker omitted to say, however, that check-cashing is lawful activity, and that the fee charged by the check casher relates directly to legitimate, valuable services provided by the check casher, including, importantly, providing liquidity to its customers days (and in some instances, up to a week) earlier than a traditional bank, which often require their customers wait for deposited checks to “clear.” This several-day difference is meaningful to, for example, construction contractors, who often require immediate cash to purchase and take delivery of building supplies and equipment, and to pay subcontractors and workers who require payment up front before beginning work. Other customers use check-cashing companies because they cannot afford bank accounts at traditional banks or have poor credit. Check cashers provide such customers the ability to cash checks, pay bills electronically, and wire money when they would otherwise be unable to do so without a bank account. All of these activities are lawful, and recognized as such, and check cashers have been publicly acknowledged as a vital source of financial services to lower income sectors of the economy. *See* 3 NYCRR 400.14 (“The legislature hereby finds and declares that check cashers provide important and vital services to New York citizens . . .”).

Agent Snedeker also presented statistics in an opaque way to misleadingly suggest that the business was routinely violating the law. According to Agent Snedeker, in 2011, Kayla processed approximately \$97 million in cash transactions but “only filed \$24 million in CTRs,” thereby suggesting that Kayla failed to file CTRs – *i.e.*, broke the law – on millions of dollars’

worth of transactions. Siegal Aff., Ex. 1 at ¶ 30. He posited that \$200,000 per day was unreported, suggesting that a large portion of Kayla's business required CTRs that were going unfiled. But Agent Snedeker did not include in his analysis that Kayla had eight separate storefronts at the time that, in the aggregate, handled approximately 400 transactions per day. If each store averaged more than four customers per day – which they did – then the average transaction amount would be below \$10,000, none of which would require a CTR filing.

Agent Snedeker's Affidavit also stated that a cooperating witness ("CW") told him that Kayla's employees "instruct many of their customers how to intentionally evade CTR filing requirements." *Id.* at ¶ 12. As a part of an undercover operation, on a handful of occasions between February 2012 and September 2012, the CW went to Kayla to cash checks. *Id.* at ¶¶ 13-17. The CW interacted directly with essentially only one of two people – Mr. H. and Mr. C.⁴ Mr. H., a salesman for Kayla, employed his own, independent staff, one of which was Mr. C.

Typically, the CW placed a call to Kayla's main telephone number and asked to speak with either Mr. H. or Mr. C. The CW told Mr. H. or Mr. C. that he planned to come to Kayla with a given amount of checks, and then went to Kayla to cash them. The Snedeker Affidavit recounts the following:

- In February 2012, the CW went to Kayla and asked Mr. C. "the best way" to deposit approximately \$17,000 in checks, and Mr. C. advised him that the "safest" way to avoid triggering reporting requirements was to break up the transaction over two days. *Id.* at ¶ 13.
- In July 2012, the CW went to Kayla and asked Mr. C. if he could cash \$14,000 in checks in a single transaction, and Mr. C. says that he has to ask his boss. *Id.* at ¶ 15. After Mr. C. speaks to someone in the back room, he returns with the cash for the CW. *Id.*
- In August 2012, the CW called Mr. C. and asked if he could cash nearly \$13,000 in checks, and Mr. C. responded that he would have "two envelopes like last time." *Id.* at ¶ 17.

⁴ Pursuant to Fed. R. Crim. P. 49.1 the identities of these individuals have been kept anonymous.

- This pattern continued until the end of September 2012. *Id.*

But the Affidavit did not provide the Magistrate Judge with the full picture. That is, the following additional details, which were omitted from the Snedeker Affidavit, are *also* readily apparent from the undercover footage produced in discovery:

- On August 30, 2012, which was not described in the Snedeker Affidavit, Mr. H. walked into the lobby and told the CW that “I can do it for you every once in a while, but sometimes when my boss is here, you know...” Siegal Aff. ¶ 9. A CTR was filed for that transaction, which the Snedeker Affidavit admits (albeit 12 paragraphs after discussing the CW’s operation specifically), when stating that Kayla filed only one CTR for the CW. Siegal Aff., Ex. 1 at ¶ 29.
- On September 12, 2012, which was also not described in the Snedeker Affidavit, Mr. C. escorted the CW to the parking lot, where he said, “it’s just different when the uh, when the boss is in. It gets tough. That’s why it took so long. He’s double checking, he wants things signed [and] he wants it done the right way. I don’t do things the right way, you know what I mean? [laughter] Alright, take care. Anytime I can help.” Siegal Aff. ¶ 10 (emphasis added.)
- On September 25, 2012, which was also not described in the Snedeker Affidavit, Mr. C. told the cooperating witness that “*when my boss is not in*, not a problem.” *Id.* ¶ 11 (emphasis added).

The Snedeker Affidavit, therefore, emphasized cherry-picked portions of the undercover footage, but omitted to describe other undercover footage that would tend to paint a different story, and one that would tend to exculpate the “boss” (*i.e.*, John). See Siegal Aff., Ex. 1 at ¶ 12.

The Snedeker Affidavit also averred that over the course of the 2006 to 2012 period, Kayla failed to file CTRs for several other customers who, at the time of the Affidavit, were the subject of the IRS’s investigation. Again seeking broadly to implicate Kayla via guilt-by-association, Agent Snedeker stated that, “[t]hese customers all used Kayla to generate cash to fund their off-the-books payroll and other unrecorded expenses.” *Id.* at ¶ 19. Among those customers are four individuals who are either under investigation for tax fraud or who pleaded guilty to tax fraud. But notably, the Snedeker Affidavit did not even purport that any Kayla

employee assisted them in structuring their transactions to avoid triggering CTR filings. *Id.* at ¶¶ 24-27. The Affidavit also failed to inform the Magistrate Judge that *CTR*s were filed on *transactions for these four customers* during the periods referenced by Agent Snedeker.

Agent Snedeker also misleadingly describes Kayla's activity for one customer, with initials "J.G.," who cashed more than \$2 million in checks at Kayla, *id.* at ¶ 22, and suggests that as a result of structuring, CTRs were filed on less than \$711,000. *Id.* Agent Snedeker added that Kayla did not file SARs on any of the transactions. *Id.* at ¶ 22. Importantly, the Snedeker Affidavit omitted the following, contradictory information: (1) Kayla filed 60 CTRs regarding Greenfield's transactions (*see Siegal Aff., Ex. 6.*); (2) these CTRs covered *more than \$1.1 million of the \$2 million in transactions*, not "less than \$711,000," as Snedeker attested (*see id.*); and (3) contrary to the suggestion that Kayla's failure to file SARs was some evidence of wrongdoing, in point of fact, the law *does not require* Kayla -- a check-cashing company, *to file SARs. See MSBs Subject to SAR Requirement, available at* <https://www.fincen.gov/msbs-subject-sar-requirement> *("[t]he SAR requirement does not apply to the following types of [money services businesses]: Check casher...")*

2. Specifying Documents to Be Seized

The Snedeker Affidavit purported to provide some specificity regarding the types of records to be seized and procedures for the searches and seizures of computer systems. *See Siegal Aff., Ex. 1 at ¶¶ 32-43.* Though Agent Snedeker requested a warrant to search for items listed in "Attachment A" for records from December 2008 to the present (*see id.* at p. 23) ("Wherefore" clause), there is no "Attachment A" to the Affidavit – that is, *nothing* is actually attached to the Affidavit itself. Moreover, the attachment to the Kayla Warrant – which is also labeled "Attachment A" – purports to cover records between January 2010 and the present.

From the materials provided to the defense, there is simply no way to tell whether the scope of the Kayla Warrant actually matches what the Magistrate Judge was asked to approve.

The Snedeker Affidavit also set forth provisions for handling computer evidence.

Premised on the notion that such devices have the capacity to store so much information in such complex ways that it would be impractical and forensically unsound to search them “on-site,” Agent Snedeker sought permission to seize or copy the computers and electronic media in their entirety, with the copy remaining with the Government for “later review.” *See id.* at ¶¶ 38-43.

Agent Snedeker explained that the analysis of the data might entail one or more of several different techniques, *not limited to*: surveying file directories and the individual files they contain; opening and reading the first few pages of files to determine their contents; scanning storage areas to discover and recover deleted files, as well as to identify deliberately hidden files; and running searches through all computers and media to determine whether a given file relates to the “subject matter” of the investigation. *Id.* at ¶ 42. In sum, Agent Snedeker asked to copy Kayla’s computers and electronic media so that the Government could search for, open up, and review every file.

The Snedeker Affidavit nowhere described how the IRS intended to distinguish information responsive to the warrant from unresponsive material (though arguably, anything on a computer, like an employee’s personal to-do list, could fit into several of the incredibly expansive categories enumerated in Attachment A to the Kayla Warrant, as described below). While Agent Snedeker articulated an intent to return “input/output peripheral devices, system software, and pertinent computer-related documentation” that are “no longer necessary to retrieve and preserve the evidence” within “a reasonable time,” *see id.* at ¶ 43, nothing in the

Snedeker Affidavit addressed how non-responsive material would be treated, whether it would be retained (and if so, for how long), and how it would be returned or purged (and if so, when).

B. The Kayla Warrant

On July 29, 2013, Magistrate Judge William D. Wall approved the Kayla Warrant. Notably, the Kayla Warrant on its face does not specify the crimes under investigation. No statute is referenced on its face. No type of crime is substantively described or even hinted at. Attached to the Kayla Warrant as “Attachment A” was a list of 10 categories of items to be seized. Like the Kayla Warrant itself, Attachment A also fails to specify a code section, nor does it provide a substantive description of any crime(s) under investigation that were to be the subject matter of the search. Paragraph 10 of Attachment A highlights the problem of a missing subject-matter description, referring (cryptically) to the “illegal transactions described herein.” Siegal Aff., Ex. 2 at ¶ 10. But that reference is to *nothing*. Nothing on the face of the Kayla Warrant, nor anything on Attachment A, provides any hint of any “illegal transactions” that are the purported subject of the investigation, or that might serve as a guide to the agents executing the search. There is no suggestion that what is to be seized should be, “related to,” for example, “satisfying Bank Secrecy Act reporting requirements” or “attempting to structure transactions.” No other documents were attached to the Kayla Warrant or incorporated by reference therein.

Attachment A to the Kayla Warrant sets out 10 general categories of records kept at most financial institutions, irrespective of their relationship to any alleged criminal activity. Every conceivable type of document or file that would be kept at a check-cashing institution is catalogued. For all practical purposes, the lists on Attachment A amounted to a *de facto* authorization to seize virtually every record of Kayla – *i.e.*, a general warrant. Attachment A seeks broad categories of records, and then further expands what may fall into each category, as follows:

- Records, documents and materials *regarding the identity of the corporate customers of Kayla, including, but not limited to*, customer lists, customer files, notes, date books, calendars, phone books, Rolodexes, or ledgers that reference customers, corporate certifications or similar documents, correspondence between Kayla and its customers, and other records, documents and materials concerning or reflecting the identity of the individual representatives of Kayla's customers, including, but not limited to, addresses, social security numbers, driver's licenses, driver's license numbers, tax identification numbers, and telephone numbers. (Siegal Aff., Ex. 2 at ¶ 1) (emphasis added)
- Records, documents and materials *that memorialize or reflect financial transactions between Kayla and its customers, including but not limited to*, logs, books, checks, receipts, invoices batch reports, bank statements, deposit slips, deposit records, notes, ledgers, cash pay out journals or records, and other records regarding the receipt of checks from customers and the pay-out of cash to customers; (*Id.* at ¶ 2) (emphasis added)
- Records, documents and materials *that memorialize or reflect financial transactions between Kayla and its source(s) of cash, including, but not limited to*, contracts, receipts, invoices, letters, bank statements, notes, ledgers, cash receipt journals or records, cash shipment records, and/or cash delivery records; (*Id.* at ¶ 3)
- Rolodexes, diaries, books, employment records, and/or identification documents regarding the identities of Kayla's employees, *or which may reflect the identities of persons affiliated with the illegal transactions described herein or who may have knowledge of facts material [to] such transactions.*" (*Id.* at ¶ 10)

Attachment A to the Kayla Warrant does not explicitly reference computers or electronic media, much less provide the searching agents with any instructions on how to seize electronic evidence, or how to handle, process, or review such evidence once seized or copied.

C. The Execution of the Search of Kayla

Around 6:00 p.m. on August 6, 2013, a team of IRS agents executed a search of Kayla. A Kayla employee called John, who was not present at the office at that time, to alert him to the fact that the IRS had shown up with a search warrant. Drago Aff. ¶ 4. John arrived at Kayla later that evening, and upon his arrival, John requested to see, and was shown, the Kayla Warrant, which he then reviewed. *Id.* ¶ 5. Confused by its lack of specificity, John asked an agent why the IRS was searching Kayla. The agent replied (in sum and substance), "It's in the

Warrant.” *Id.* John responded that he did not see any crime described in the Kayla Warrant, at which point the agent took the Kayla Warrant from John, reviewed it himself, appeared concerned, and voiced an expletive, and then told another agent words to the effect of, “it’s not in here.” *Id.* That other agent, too, then looked at the Kayla Warrant and hastily exclaimed aloud: “BSA violations.” *Id.* Despite this exchange and the Agents’ contemporaneous awareness of the Kayla Warrant’s facial defects, they proceeded to search unabated for the next several hours. *Id.*

The IRS seized virtually every piece of paper that bore the name of a customer, employee, or Kayla itself, as well as copies of hard drives from 11 computers and one flash drive. *See Siegal Aff., Ex. 3.* Similarly, the electronic devices (or electronic “image” copies of them) were permanently retained by the IRS. (An electronic copy of one hard drive was given to John and Kayla in 2016). To date, defense counsel has not received any discovery from the electronic devices, and in conversations with defense counsel over the last month, the Government has not made clear what, if any, information it intends to “use” from the seized electronic devices at trial. It remains unclear, however, to what “use,” if any, that electronic evidence has *already* been put by the Government in the five years since it was seized.

D. After the August 2013 Search

At the time the search was executed, neither John nor the business was charged with any crimes. Approximately five years later, in, what appears to have been a last minute scramble, the Government obtained the Indictment in this case on July 31, 2018 (the “Indictment”). John was arrested at his home on August 1, 2018.

Upon John’s arrest, he was escorted by an IRS agent from the downstairs area of his house to his upstairs bedroom. After an agent asked John if he wanted to call his attorney, the agent walked to the opposite side of John’s room to grab a cell phone – a Samsung Galaxy S9

phone – from John’s nightstand. The agent then brought the phone to John and handed it to him, and John called his attorney. Another agent then instructed John to hand over the the cell phone. John asked if they had a warrant for it. One agent said words to the effect that no warrant was necessary because the phone was “on his (John’s) person.” Another agent said words to the effect that they already had a warrant for the phone. The agents then took the cell phone from John, *see* Drago Aff. ¶ 7, and have retained it ever since.⁵ As it turned out, no warrant for the phone had yet been obtained, as described more fully below.

Shortly thereafter, John was transported to the courthouse by one of the agents whom John recognized from the search of Kayla’s offices five years earlier. The agent recognized John and commented, “you are the guy from five years ago. They’re just doing this now?” *Id.* ¶ 8.

E. The Indictment

The Indictment charges John with violations of the BSA as well as violations of the Internal Revenue Laws. Tellingly, the charges appear to be based almost entirely on information known to the Government either at the time of, or before, the search of Kayla in 2013.

The Indictment’s BSA allegations against John largely reflect the allegations explained in the Snedeker Affidavit five years earlier, but instead of being attributed to Kayla or its employees, are lodged solely against John. These include Counts One, Two, and Three.

Count One concerns John’s alleged failure to file CTRs. According to the Indictment, “[o]n or about and between January 1, 2010 and October 31, 2013,” John knowingly and willfully caused Kayla to fail to file *one or more* CTRs as part of a pattern of illegal activity involving more than \$100,000 in a 12-month period. Indictment ¶ 17. The Indictment does not

⁵ By letter dated November 21, 2018, the Government informed counsel that (at least as of that date) the Government had not yet been able to access John’s cell phone.

provide any further detail on which CTRs allegedly should have been (but were not) filed, such as the date(s), customer(s), or amount(s) in question.

Count Two concerns John's alleged failure to develop, implement, and maintain an effective AML program at Kayla. The Indictment alleges that between August 1, 2010 and October 31, 2013, John knowingly and intentionally failed to implement and maintain effective policies, procedures, and controls for filing CTRs, and failed to provide adequate education and training for appropriate personnel. *Id.* ¶¶ 18-21. The Indictment generally alleges that John failed to ensure that Kayla's employees were advising customers not to structure, agreed to accommodate requests by customers not to file CTRs, failed to file CTRs, and failed to provide accurate information to Kayla's employees so that they could file CTRs. But the Indictment does not state which CTR(s) were not filed, or for whom, or when John failed to provide his employees with accurate information. *Id.* ¶ 21.

Count Three concerns John's alleged structuring. Between August 1, 2010 and October 31, 2013, the Indictment alleges that John knowingly and intentionally structured or assisted in structuring *one or more financial transactions*. *Id.* ¶ 23. As with Count One, the Indictment does not provide any further detail on the alleged structuring, including the customer(s) involved, the dates of the transactions, or the amounts.

Counts Four through Eight concern John's alleged failure to collect and pay FICA taxes between April 1, 2012 and July 31, 2013. *Id.* ¶ 25. There are no details about the employees from whom taxes were allegedly not collected or paid, the months when John allegedly failed to collect the FICA taxes, and the amount of tax alleged to be at issue.

F. The Application to Search John's Cell Phone

With John's phone in its possession, later that same day, the Government applied for a warrant to search the phone (the "Phone Warrant"). The supporting affidavit was sworn by IRS

Special Agent Heather McCue (“McCue Affidavit”). Siegal Aff. Ex. 4. That warrant application sought authorization to search for and seize John’s cell phone for evidence of violations of the “Bank Secrecy Act,” as well as violations of 18 U.S.C. §§ 371, 1343, 1349, 1956, and 1957.

As a preliminary matter, the actual Phone Warrant and its two attachments do not even match up with the McCue Affidavit or its attachments. Rather, the government seems to have simply done a sloppy cut-and-paste job from a previous application to search a different cell phone in an entirely different case. For instance, the Phone Warrant’s Attachment A described the phone to be searched as a Silver *Apple Phone*, IMEI 353254072140029 – *i.e., not* the Black Samsung Galaxy S9, IMEI 352410091613245 that was seized – belonging to someone named Nagabhushanam Bandoji (*i.e., not* John). Siegal Aff. Ex. 5.

Moreover, the search warrant affidavit listed numerous statutes that were not even part of this investigation and that are not included in the Indictment. That is, although the Indictment charges only BSA and FICA violations, the search warrant application names a bevy of statutes that were not charged in the Indictment, and for which no independent probable cause was ever established in the context of the application for it, including Title 18 U.S.C. § 371 (conspiracy) and Title 18 U.S.C. § 666 (theft or the giving or receiving of bribes). These glaring inconsistencies underscore yet again the careless nature of this search warrant application.

The preface to Attachment B in the Phone Warrant provides that the Government may search for evidence of violations of Title 18 U.S.C. §§ 371, 666, 1341, 1349, 1956, and 1957 (though Paragraph 8 references 18 U.S.C. § 1343 as well). Siegal Aff. Ex. 5. The McCue Affidavit’s Attachment B contemplates evidence of violations of Title 31 (the BSA) – which was entirely omitted from the Phone Warrant’s Attachment B – and omits any reference to 18 U.S.C. § 666 or 1341. Siegal Aff. Ex. 4 at Att. B. As with the inconsistencies between the Kayla

Warrant and the Snedeker Affidavit, there is simply no way to tell whether the scope of the Phone Warrant actually matches what the Magistrate Judge was asked to approve.

The McCue Affidavit asserted that there is probable cause to believe that John's actual phone contains evidence of several crimes, including "Bank Secrecy Act" violations, conspiracy (18 U.S.C. § 371), wire fraud (18 U.S.C. § 1343), attempt and conspiracy (18 U.S.C. § 1349), money laundering (18 U.S.C. § 1956), and engaging in monetary transactions with property derived from illegal activity (18 U.S.C. § 1957). Siegal Aff. Ex. 4. To establish probable cause, Agent McCue appeared to rely on her general "experience and training," "review of documents," "witnesses," and "discussions with other law enforcement officers." *Id.* at ¶ 3. She averred that "[d]uring the course of the investigation and from the statements made by DRAGO during the arrest, it is clear that . . . his electronic communications amongst his employees will support his knowledge and substantiate his involvement to *defraud the US Government.*" *Id.* at ¶ 10 (emphasis added).

Over the course of the scant 15-paragraph Affidavit, Agent McCue's factual allegations supporting the charges were non-existent. That is because five of these charges – everything other than the vague charges of "violations of the Bank Secrecy Act" – have nothing to do with the charges that were actually brought against John in the Indictment. That is, to the extent probable cause was impliedly established for this search by dint of the arrest warrant for John, that warrant was based on an indictment of him for BSA and tax violations, which under no circumstances could support a warrant to search his cell phone for evidence of *wire fraud, bribery, money laundering, or conspiracy.*

The McCue Affidavit also did not provide any specificity regarding the "particular things to be seized." Attachment B to the McCue Affidavit provided that the Government will *Maintain*

all information obtained from the cell phone and review “[a]ll records and information ... including names and telephone numbers, . . . the contents of all call logs, contact lists, text messages, emails . . . instant messages, photographs, videos, Facebook posts, Internet activity . . . and other electronic media . . .” Siegal Aff. Ex. 4 at Att. B (emphasis added). It then listed out eight categories of information that are included in the above categories, including “[e]vidence of user attribution” – *i.e.*, anything showing who “used” the phone. *Id.* ¶ 1. It also allowed the Government to search “when” the phone was used. *Id.* ¶ 6. Other categories of information included saved usernames and passwords, anything that indicates (or does not indicate that the phone has security software), and any “[c]ontextual information necessary to understand the evidence described in this attachment.” *Id.* ¶¶ 2-3, 7-8. The list ended with the following catch-all: “the terms[,] records and information include *all of the foregoing items... in whatever form and by whatever means.*” (emphasis added).

Finally, the type of phone the IRS seized from John – a Samsung Galaxy S9 – was not introduced to the marketplace until February 2018.⁶ That is, this type of phone *did not even exist* at the time of the Indictment’s alleged crimes (which ended no later than the end of 2013). The Galaxy S9 would not exist for more than four years after the charged events.

⁶ Arjun Kharpal, *Samsung launches the Galaxy S9 smartphone to take on Apple’s iPhone X*, CNBC (Feb. 25, 2018 1:58 PM), available at <https://www.cnbc.com/2018/02/25/samsung-galaxy-s9-launches-at-mobile-world-congress-specs-price.html>.

ARGUMENT

I.

THE IRS KNOWINGLY EXECUTED A FACIALLY UNCONSTITUTIONAL SEARCH WARRANT IN AUGUST 2013, AND ITS FRUITS SHOULD BE SUPPRESSED

The Government violated John's Fourth Amendment right to be free from unreasonable searches and seizures when, in August 2013, it searched Kayla's offices pursuant to a written warrant that was constitutionally defective on its face. The Kayla Warrant violated the "particularity" requirement of the Fourth Amendment, providing the searching officers none of the requisite guidance for what could (or could not) be seized. Lacking the required particularity, the Kayla Warrant effectively granted the searching agents unbridled discretion to seize nearly any and every piece of paper and electronic record at Kayla. And indeed, the agents did essentially just that, walking off with approximately 25 boxes of hard copy documents and the full data contents of 11 electronic devices. Worse, the facial invalidity of the Kayla Warrant *was brought to the attention of the agents at the time of the search, and acknowledged by the agents at the time*, yet the agents plowed ahead anyway, in a blatant, knowing violation of John's rights. Accordingly, the fruits of the search should be suppressed.

A. Constitutional Requirements for Search Warrants

The Fourth Amendment to the United States Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, *and particularly describing* the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV (emphasis added); *see also United States v. Galpin*, 720 F.3d 436, 445-47 (2d Cir. 2013); *Frederique v. Cty. of Nassau*, 168 F. Supp. 3d 455, 474 (E.D.N.Y. 2016) (Feuerstein, J.).

The Warrants Clause was intended as a bulwark against “the ‘general warrant’ abhorred by the colonists” and protects against “a general, exploratory rummaging in a person’s belongings.” *Coolidge v. New Hampshire*, 403 U.S. 443, 445 (1971); *see also United States v. Buck*, 813 F.2d 588, 590 (2d. Cir. 1987) (same); *Galpin*, 720 F.3d at 445 (“[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.”) (citing *Arizona v. Gant*, 556 U.S. 332, 345 (2009)). Its overarching purpose is to ensure that “those searches deemed necessary should be as limited as possible.” *Coolidge*, 403 U.S. at 467. Therefore, to prevent the “wide-ranging exploratory searches the Framers intended to prohibit,” the Fourth Amendment requires the search to be “carefully tailored to its justifications” and thus limits an officer’s authority to search only the “specific areas and things for which there is probable cause to search.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also United States v. Wey*, 256 F. Supp. 3d 355, 379-80 (S.D.N.Y. 2017) (same).

In the same vein, the Warrants Clause requires particularity and forbids overbreadth. *See United States v. Cohan*, 628 F. Supp. 2d 355, 359 (E.D.N.Y. 2009) (explaining that a warrant may violate the Warrants Clause “either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries.”); *United States v. Hill*, 459, F.3d 966, 973 (9th Cir. 2006) (“Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.”) (citations omitted). In determining whether a warrant violates the Warrants Clause particularity requirement, a court must consider: “(1) whether the items listed as ‘to be seized’ in the warrant were overbroad because they lacked probable cause and (2) whether

the warrant was sufficiently particularized on its face to provide the necessary guidelines for the search by the executing officers.” *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 450 (S.D.N.Y. 2013) (citations omitted).

Evidence obtained in an unconstitutional search, as well as the fruits of that search, are subject to suppression. *See Herring v. United States*, 555 U.S. 135, 139 (2009) (stating that the exclusionary rule “forbids the use of improperly obtained evidence at trial”); *United States v. Morris*, No. CR 07-2009 (NG) (JO), 2007 U.S. Dist. LEXIS 104248, at *14-16 (E.D.N.Y. Oct. 31, 2007) (suppressing “fruit” of the unlawful stop and seizure); *United States v. Bin Laden*, No. S(7) 98 Cr. 1023 (LBS), 2000 U.S. Dist. LEXIS 18957, at *9 (S.D.N.Y. Dec. 15, 2000) (“The rule that evidence derived from an unconstitutional search or interrogation will be suppressed as the ‘fruit of the poisonous tree’ is firmly established.”). The exclusionary rule was designed to “deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures” by preventing the Government from introducing at trial any improperly obtained evidence. *United States v. Calandra*, 414 U.S. 338, 347 (1974); *see also United States v. Berschansky*, 788 F.3d 102, 112 (2d Cir. 2015) (the exclusionary rule deters “deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.”) (quoting *Herring*, 555 U.S. at 144).

According to the exclusionary rule any evidence obtained in the search of Kayla’s offices, as well as any evidentiary fruits obtained from that evidence, should be suppressed because the warrant (1) was not particularized and was unconstitutionally overbroad; and (2) was based on an application that failed to establish probable cause. *See, e.g., United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014) (“*Ganias I*”); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (“*Ganias II*”).

B. The Kayla Warrant Fails to Describe with Particularity the Items To Be Seized

The Kayla Warrant violates the Constitution on its face, because it fails to comply with the Fourth Amendment’s requirement to describe with particularity the items to be seized. Instead, the warrant for Kayla’s office simply lists every conceivable business record that could possibly exist at a check-cashing institution. Siegal Aff., Ex. 2. Further, it utterly fails to describe the crime(s) – any crimes – under investigation, either by descriptive word(s) or reference to any code section or legal theory. *Id.* As a result, the searching officers were left entirely to their own, uninformed discretion to determine what to seize, giving them virtual *carte blanche* to seize anything in Kayla’s office that related to Kayla, its customers, or employees. This is fatal.

“The Fourth Amendment’s requirements regarding search warrants are not ‘formalities[,]’ but rather, specifically designed and enforced to prevent unreasonable and indiscriminate seizure of a person’s belongings. *United States v. Voustianiouk*, 685 F.3d 206, 210 (2d Cir. 2012) (citation omitted). Indeed, as courts have recognized, the particularity requirement aims to “prevent[] general searches, prevent[] the seizure of objects upon the mistaken assumption that they fall within the magistrate’s authorization, and [prevent] the issuance of warrants without a substantial factual basis.” *Zemlyansky*, 945 F. Supp. 2d at 452 (citing *United States v. Young*, 745 F.2d 733, 759 (2d Cir. 1984)). Warrants may not “leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized,” *United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990), but instead must “contain sufficient specificity ‘to permit the rational exercise of judgment [by the executing officers] in selecting what items to seize.’” See *Zemlyansky*, 945 F. Supp. 2d at 453; see also *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000). The particularity requirement’s purpose is “not

limited to the prevention of general searches” – it also “assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.” *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citation omitted).

Though “there is no settled formula for determining whether a warrant lacks particularity,” *Zemlyansky*, 945 F. Supp. 2d at 453, courts in this Circuit have noted that “two factors . . . above others, tend to define a warrant’s insufficient particularity[:]”

First, warrants are generally found to be insufficiently particular where [n]othing on the face of the warrant tells the searching officers for what crime the search is being undertaken. Second, warrants will frequently lack particularity where they include a general, catch-all paragraph or provision, often one authorizing the seizure of any or all records of a particular type.

United States v. Vilar, NO. S3 05-CR-621 (KMK), 2007 U.S. Dist. LEXIS 26993, at *66-67 (S.D.N.Y. Apr. 4. 2007) (internal citations omitted); *see also United States v. DiScala*, 14-cr-399 (ENV), 2018 U.S. Dist. LEXIS 36817, at *52-53 (E.D.N.Y. Feb. 27, 2018). But a defendant need not show both of these shortcomings to prove that a warrant lacks particularity – “rather, one or the other will typically render a warrant unconstitutional.” *Zemlyansky*, 945 F. Supp. 2d at 453; *see also United States v. Gigante*, 979 F. Supp. 959, 966 (S.D.N.Y. 1997) (finding a general warrant where the warrant authorized seizure of all “financial, banking, safe deposit, investment, asset, tax, bookkeeping, and accounting records”); *United States v. Bianco*, 998 F.2d 1112, 1116 (2d Cir. 1993) (warrant lacked particularity where it did not describe “the possible crimes involved”); *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992) (holding warrant insufficiently particular where “[n]othing on the face of the warrant tells the searching officers for what crime the search is being undertaken”). Here, the Kayla Warrant suffers from both deficiencies.

First, the Kayla Warrant fails to identify the crime(s) under investigation. *See Vilar*, 2007 U.S. Dist. LEXIS 26993 at *66. Critically, no criminal code section is referenced anywhere on the Kayla Warrant or on Attachment A. Nor is any criminal behavior substantively described. Notably, the language of the Kayla Warrant appears to acknowledge the need to reference some identifiable form of criminal behavior, yet then, inexplicably, fails to do so: it makes a passing reference to “the illegal transactions described herein” but nowhere “therein” (or anywhere else) describes *any* form of illegal transaction.⁷ Nor does the Kayla Warrant attach an affidavit or incorporate one by reference, to describe any form of illegal activity under investigation. The Kayla Warrant and its Attachment A simply list types of documents related to financial transactions, employees, customers, and responsibilities of a financial institution – in other words, covering, effectively, virtually any document that would be found at a business like Kayla. No agent reviewing the Kayla Warrant or its attachment could reasonably determine what should be seized as relevant to some unspecified crime, and what should not, from the face of the Kayla Warrant. This failure to specify the crime(s) under investigation, in and of itself, renders the Kayla Warrant insufficiently particular and unconstitutionally invalid.

It bears noting that the Government cannot rely on the contents of the Snedeker Affidavit submitted in the application for the Kayla Warrant to save the Warrant from its shortcomings. The warrant must stand on its own, because “supplementary documents, including affidavits” can particularize a warrant “*only if attached and incorporated into the warrant by reference.*” *Zemlyansky*, 945 F. Supp. 2d at 453; *see also United States v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010) (“we may no longer rely on unincorporated, unattached supporting documents to cure an

⁷ This phrase cannot suffice to save the warrant. *See United States v. George*, 975 F.2d 72, 75-76 (2d Cir. 1992) (warrant permitting seizure of evidence “relating to commission of a crime” held constitutionally infirm because “[n]othing on the face of the warrant tells the searching officer for what crimes the search is being undertaken.”).

otherwise defective search warrant"); *see also Groh*, 540 F. Supp. at 557 ("[t]he fact that the application adequately described the 'things to be seized' does not save the warrant from its facial invalidity" because the Fourth Amendment "by its terms requires particularity in the warrant"). As the Second Circuit has concluded, "for an attached affidavit properly to be incorporated into a warrant, the warrant must contain 'deliberate and unequivocal language of incorporation'" – "[l]anguage in a warrant that simply references an underlying affidavit" does not suffice." *See Wey*, 256 F. Supp. 3d at 382 (quoting *650 Fifth Ave. v. Alavi Found*, 830 F.3d 66, 98 (2d Cir. 2016) (internal quotation marks omitted)). Of course, the Kayla Warrant neither attaches nor references the Snedeker Affidavit.

Any agent who looked at the face of this warrant ought to have realized that this was a general warrant and that it lacked constitutionally-required particulars. *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011).⁸ Amazingly, this fatal flaw in the warrant *was known to the searching agents* at the time of the execution of the search, yet willfully ignored by them as they pressed ahead with their unconstitutional search. While the language making empty reference to "the illegal transactions described herein" – which were not so described – suggests the agents actually knew in advance that the warrant should have had such a description, it gets worse. At some point shortly after the agents arrived on the scene to execute the warrant, John was presented with the Kayla Warrant. Drago Aff. ¶ 5. After reviewing it, John asked the agents why Kayla was being searched and pointed out to the agents that no crimes were described in the Kayla Warrant. *Id.* In response, one agent replied with an expletive, demonstrating his

⁸ The Government simply cannot "reasonably rely" on an insufficiently particularized warrant. *See Buck*, 813 F.2d at 593 n.2; *George*, 975 F.2d at 77-78 (holding a warrant that allows the seizure of materials "without mentioning a particular crime or criminal activity to which the evidence must relate is void under the Fourth Amendment," and cannot be relied on in good faith); *Zemlyansky*, 945 F. Supp. 2d at 454, 457; *United States v. Cioffi*, 668 F. Supp. 2d at 392; *Vilar*, 2007 U.S. Dist. LEXIS 26993, at *76-77; *United States v. Rollack*, 90 F. Supp. 2d 263, 274, 277 (S.D.N.Y. 1999); *see also United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995); *United States v. Leary*, 846 F.2d 592, 602-10 (10th Cir. 1988).

acknowledgment that the warrant was indeed missing this critical information. *Id.* Another agent who also recognized the problem in real time, then attempted to orally supply his own view of the Kayla Warrant’s coverage, exclaiming “BSA violations,” (or words to that effect).⁹ *Id.* Of course, having observed and acknowledged the serious problem with the Kayla Warrant, the agents could have halted the search and called the AUSA and sought to obtain a warrant that did comport with the law. Instead, after realizing that the warrant was void, the agents pressed ahead nonetheless.

Second, the Kayla Warrant impermissibly authorizes the seizure of any and all records. Attachment A to the Kayla Warrant lists every conceivable type of document or file that would be kept at a check-cashing institution, effectively giving the searching officers free reign to seize any and all files fulfilling one of several broad criteria, *irrespective of whether the files were related to some crime*, including documents regarding “the identity of corporate customers of Kayla,” “financial transactions between Kayla and its customers,” and “financial transactions between Kayla and its source(s) of cash.” For instance, Paragraph 1 of Attachment A provides that the searching officers may seize “[r]ecords, documents, and materials regarding the identity of the corporate customers of Kayla, *including, but not limited to*, customer lists, customer files, notes, date books, calendars, phone books, Rolodexes, or ledgers that reference customers, corporate certifications or similar documents, correspondence between Kayla and its customers;

⁹ Even if “BSA violations” had been written into the warrant itself, in all likelihood that would be insufficient to satisfy the Particularity requirement, given that the “BSA” – *i.e.*, the Bank Secrecy Act – can be understood to cover myriad provisions encompassing all sorts of regulatory and criminal provisions contained both in the criminal code and hundreds, if not thousands, of regulations promulgated thereunder. 31 U.S.C. §§ 5311-5332. As several courts have made clear, “even warrants that identify catch-all statutory provisions, like mail fraud or conspiracy statutes, may fail to comply” with the particularity requirement. *Galpin*, 720 F.3d at 445, n.5; *see also United States v. Leary*, 846 F.2d 592, 594 (10th Cir. 1988) (warrant authorizing search of company’s business records for violation of “Arms Export Control Act, 22 U.S.C. § 2778, and the Export Administration Act of 1979, 50 U.S.C. App. § 2410,” held overbroad); *United States v. Roche*, 614 F.2d 6, 8 (1st Cir. 1980) (holding that “limitation” of a search to evidence relating to the general mail fraud statute, 18 U.S.C. § 1341, provides “no limitation at all”).

and other records, documents and materials concerning or reflecting identity of the individual representatives of Kayla’s customers, including, but not limited to, addresses, social security numbers, driver’s licenses, driver’s license numbers, tax identification numbers, and telephone numbers.” Siegal Aff., Ex. 2 at ¶ 1. Whether specifically enumerated or not, pursuant to this description, the officers could have seized anything with any name on it other than Kayla, whether specifically listed above or not. *See, e.g., United States v. SDI Future Health, Inc.*, 568 F.3d 684, 705 (9th Cir. 2009) (“Category 24 – SDI’s rolodexes, address books, and calendars -- amounts to the laziest of gestures in the direction of specificity . . . [t]his category practically begs the search team to find and to seize the contact information of every person who ever dealt with SDI”). The instructions of this Paragraph of the warrant are essentially limitless.

Other paragraphs on Attachment A similarly target every form of document or thing imaginable that would be maintained at a business. For example, Paragraph 2 to Attachment A, covered materials “*including but not limited to*, logs, books, checks, receipts, invoice batch reports, bank statements, deposit slips, deposit records, notes, ledgers, cash pay out journals or records, and other records regarding the receipt of checks from customers and the pay-out of cash to customers” – *i.e.*, anything maintained in Kayla’s ordinary course of business. *Id.* at Att. A. ¶ 2. Likewise, Paragraph 6 sought “[*all*] logs or lists referencing *all* currency transaction reports or similar reports . . .” without defining what similar reports are or providing any sort of limitation on what might be relevant. *Id.* ¶ 6 (emphasis added). What this means, practically speaking, is that the searching officers could have picked up anything that even somewhat resembled a “report” and taken it – regardless of its content.

Courts in this Circuit have routinely held that similarly expansive categories of documents render warrants constitutionally deficient. *See Bianco*, 998 F.2d at 1115-16 (warrant

for home authorizing seizure of “[n]otes, [l]edgers, [e]nvelopes, [p]apers and [r]ecords containing [i]nitials, [n]ames, [a]ddresses, [d]ollar [a]mounts, [c]odes, [f]igures, and the like” was insufficiently particularized especially when such items were not “tied to particular crimes”), *abrogated on other grounds by, Groh v. Ramirez*, 540 U.S. 551 (2004); *Buck*, 813 F.2d at 591 (holding that warrant was insufficiently particularized where it consisted entirely of “general boilerplate terms, without either explicit or implicit limitation on the scope of the search”); *United States v. Hickey*, 16 F. Supp. 2d 223, 237-41 (E.D.N.Y. 1998) (warrant authorizing seizure of “all business records” of four companies, “including but not limited to” approximately 50 individually listed generic terms, was deficient); *Gigante*, 979 F. Supp. at 966 (warrant permitting seizure of “financial, banking, safe deposit, investment, asset, tax, bookkeeping, and accounting records” along with “underlying, supporting, and related documentation,” of “or referring or relating to” named individuals lacking particularity).

Although some meaningful limitation could theoretically salvage the Kayla Warrant, any such limitations are notably absent. In fact, nearly every category of documents (each of which is impermissibly broad) is accompanied by some broad language that expands – rather than restricts – what documents can be seized. Such “catch-all” language, “without, crucially, any linkage to the suspected criminal activity, or indeed any meaningful content-based parameter or other limiting principle,” further supports the conclusion that the Warrant is insufficiently particularized. *See Wey*, 256 F. Supp. 3d at 385-86 (concluding that “even the most specific descriptions” . . . (e.g., ‘documents concerning or reflecting the movement of funds,’ ‘checks,’ ‘transaction records,’ ‘Rolodexes,’ ‘diaries,’ ‘calendars,’ etc.’) are all “fairly general”) (citations omitted).

The catch-all language in these paragraphs becomes even more problematic given the absence of any specified criminal conduct, as such language prevents an agent from “distinguishing meaningfully between materials of potential evidentiary value and those devoid of it.” *See id.*, at 386. Conferral of such “unfettered discretion . . . particularly in light of the [Warrant’s] independent failure to identify any crime under investigation, is inconsistent with the Fourth Amendment’s particularity requirement.” *Id.* at 387.

The search and seizure of computers presents an additional problem. In the context of electronically stored information, the particularity requirement “assumes even greater importance.” *Galpin*, 720 F.3d at 446. This is because a computer may hold information entirely unrelated to the criminal investigation that led to the seizure and “can give the government possession of a vast trove of personal information about the person to whom the drive belongs.” *Ganias II*, 824 F.3d at 217. As courts in this Circuit have stressed, “the Government, once it has obtained authorization to search a hard drive, may in theory ‘claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant.’” *Wey*, 256 F. Supp. 3d at 373. This presents a “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.” *Galpin*, 720 F. 3d at 447 (citation omitted); *Ganias II*, 824 F.3d at 231 (Chin, J., dissenting) (nothing that “[v]irtually all the entirety of a person’s life may be captured as data” on a smartphone or computer); *Cioffi*, 668 F. Supp. at 391 (“The dawn of the Information Age has only heightened [privacy] concerns. The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because ‘[c]omputers . . . often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize.’”) (citation omitted).

This is particularly relevant here, where the Government created copies of 11 computers (and retained these copies) presumably under the assumption that the computers housed files within the scope of Attachment A. Thus, the Government could search for any of several broad categories of documents, including for information related to employees or customers, regardless of whether the Government had reason to believe they are implicated in any sort of criminal activity. For instance, Paragraph 7 authorizes the seizure of “[r]ecords, documents and materials that contain data” used to prepare CTRs, which effectively gives the Government access to *anything* – not just CTRs or other reports – that contains any customer’s personal information – like home addresses or social security numbers – because such information is used to file a CTR. Siegal Aff., Ex. 2 at Att. A at ¶ 7. Moreover, Paragraph 10, which allows the Government to search for any documents regarding the identity of Kayla’s employees, purports to give the Government the right to view personal files, entirely unrelated to an employee’s job, if the employee saved a file on her work computer.

These are precisely the types of searches that the Fourth Amendment intends to prevent. See *United States v. Fleet Mgmt. Ltd.*, 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007) (holding that “any and all data . . . including but not limited to” a list of items was sufficient to render a computer search warrant unconstitutional); see also *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009), cert. denied, 557 U.S. 924 (2009) (stating that the ability of a computer to store “a huge array” of information “makes the particularity requirement that much more important” and noting that a warrant authorizing the seizure of “any and all information and/or data” fails the particularity requirement); *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (concluding that warrant to seize “[a]ll other computers” was not sufficiently particular where description “did not indicate the specific crimes for which the equipment was sought, nor were

the supporting affidavits or the limits contained in the searching instructions incorporated by reference.”). The overwhelming breadth of the computer search parameters, in and of themselves, merits a finding that the Kayla Warrant violated John’s Fourth Amendment rights.

To the extent there is any doubt from the face of the Kayla Warrant that it is unconstitutionally lacking in particularity, the IRS’s execution of the warrant conclusively drives this point home. Among the 20-odd boxes of hard copy materials, the agents seized, *e.g.*, records of utility payments and Department of Motor Vehicle records for a separate store, which were plainly apparent from the labeling of the files seized (*e.g.*, “Uniondale – Utilities”), as well as daily activity reports from “Mid Island” – the predecessor to Kayla of nearly 20 years earlier. The Kayla Warrant left the agents to their own, unfettered discretion in electing what was subject to seizure – and as a result, they just swept it all up.

C. The Kayla Warrant Is Overbroad and Lacks Probable Cause

The Constitution limits law enforcement’s rights to search only “the specific areas and things for which there is probable cause to search,” and requires “that the search . . . be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” *Garrison*, 480 U.S. at 84. A search warrant is impermissibly overbroad when it includes items for which there is no probable cause. *See United States v. Criminal Triumph Capital Grp.*, 211 F.R.D. 31, 59 (D. Conn. 2002). The Kayla Warrant was impermissibly overbroad because Attachment A does not provide any meaningful guidance to the searching officers to determine how to discern between evidence of the suspected crime(s) – *i.e.*, the crime(s) described in the application paperwork – and materials kept in the ordinary course and not suspicious on their face. As a result of the overly broad sweep of the warrant’s language, the officers were effectively left to fish through and seize virtually every

business record and electronic storage device (and the contents thereof) at Kayla, including records for which no probable cause was ever established.

In determining whether a warrant is constitutionally overbroad, courts consider whether probable cause exists “to support the breadth of the search that was authorized.” *United States v. Scully*, 108 F. Supp. 3d 59, 90 (E.D.N.Y. 2015) (quoting *United States v. Dinero Express, Inc.*, No. 99 Cr. 975 (SWK), 2000 U.S. Dist. LEXIS 2439, at *25 (S.D.N.Y. Mar. 1, 2000)). The probable cause standard is met where “the totality of circumstances indicates a ‘fair probability that contraband or evidence of a crime will be found in a particular place.’” *Walczuk v. Rio*, 496 F.3d 139, 156 (2d Cir. 2007) (citation omitted). To permit search and seizure of “fairly broad” materials, the affidavit in support must “provide[] the necessary basis for a determination of probable cause to seize items in each of these categories.” *Zemlyansky*, 945 F. Supp. 2d at 464. “[A] warrant is overbroad if its ‘description of the objects to be seized … is broader than can be justified by the probable cause upon which the warrant is based.’” *United States v. Lustyik*, 57 F. Supp. 3d 213, 228 (S.D.N.Y. 2014) (quoting *Galpin*, 720 F.3d at 446); see also *United States v. Conley*, No. 3:17-CR-214, 2018 U.S. Dist. LEXIS 160511, at *47 (D. Conn. Sept. 20, 2018) (“[A]n unparticularized description of the items subject to search under a warrant may result in the warrant exceeding the scope of the established probable cause.”).

When the type of property is “generally in lawful use in substantial quantities,” even “[g]reater care in description [i]s … called for.” *Wey*, 256 F. Supp. 3d at 385 (quoting 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.6(a) (5th ed. 2012)) (also noting that “[a] more particular description than otherwise might be necessary is required when other objects of the same general classification are likely to be found at the particular place to be searched”); cf. *United States v. Morisse*, 660 F.2d 132, 136 n.1 (5th Cir. 1981) (if the

“nature of the [suspected illegal] activity does not allow for [the] ready segregation” of illegal items from “legal items,” then “the magistrate should take care to assure the warrant informs the law enforcement agent as to how he should distinguish between the illegal paraphernalia and the items that are held legally.”)

No such description was provided here. The Snedeker Affidavit (which was not attached to the Kayla Warrant) simply did not establish probable cause to seize all the documents and things covered by the words on the face of Attachment A, as discussed more fully below. Rather, the Snedeker Affidavit suggested, at most, grounds to seize documents related to certain identified customers of Kayla (*i.e.*, not all its customers), including records of transactions involving those customers and any reports filed for those customers, and perhaps other related financial records. Agent Snedeker’s attestations simply did not support the search and seizure conducted pursuant to the Kayla Warrant.

Critically, Attachment A to the Kayla Warrant sets forth expansive categories of generic items subject to seizure without any link to the suspected criminal activity, because as stated above, the Kayla Warrant does not provide any citation to any criminal code or provide any insight into the alleged crime. This failure, practically speaking, authorizes the Government to seize documents related to any financial activity (all of which are kept or maintained in the ordinary course at a check-cashing institution) irrespective of their link to (some unspecified) criminal activity. That failure allowed agents to indiscriminately seize anything from Kayla – irrespective of probable cause – eviscerating the standard that there be a “fair probability” of evidence of a crime in a given item to be seized, and instead allowing agents to employ their own “any conceivable link to any conceivable crime” standard in determining what to take.

For instance, Paragraph 3 of Attachment A authorizes seizure of “[r]ecords, documents and materials that memorializes or reflect financial transactions between Kayla and its source(s) of cash, *including, but not limited to*, contracts, receipts, invoices, letters, bank statements, notes, ledgers, cash receipt journals or records, cash shipment records, and/or cash delivery records.”

Siegal Aff., Ex. 2 at Att. A. at ¶ 3 (emphasis added). Nowhere in the Attachment itself is there any allegation of a crime involving one of Kayla’s “sources of cash” or even a suggestion as to why such records could possibly reflect evidence of a crime. Nor is there any mention of a crime in the Snedeker Affidavit that could conceivably be evidenced in records reflecting Kayla’s sources of cash. There simply is no meaningful limit as to what items may or may not be seized pursuant to this category, which, by the Government’s failure to include any sort of guidance to the executing officers, renders it overbroad.

Similarly, Paragraph 10 of Attachment A authorizes the seizure of “[r]oledexes, diaries, books, employment records, and/or identification documents regarding the identity of Kayla’s employees, *or which may reflect the identities of persons affiliated with the illegal transactions described herein or who may have knowledge of facts material [to] such transactions.*” Siegal Aff., Ex. 2 at Att. A at ¶ 10 (emphasis added).¹⁰ Construing the first part of the Paragraph most favorably to the Government, it authorizes seizure of any record, including those with personally identifiable and potentially sensitive information, related to any Kayla employee – past or present. The additional language authorizing seizure of any document “which may reflect the identities of persons affiliated with the illegal transactions described herein or who may have

¹⁰ As with Paragraph 3, the Snedeker Affidavit provided no basis whatsoever to suggest that any employment record of Kayla would reflect evidence of a crime. Indeed, in its description of the investigation and probable cause, the Snedeker Affidavit relies primarily on the bad acts of two individuals – Mr. C. (whom the affidavit mistakenly characterizes as a Kayla employee) and Mr. H. – who it alleged were involved with the alleged failures to file CTRs and structuring. Paragraph 10 of the Warrant is not limited to records concerning those individuals, however, and instead authorizes seizure of any document with any name on it.

knowledge of facts material [to] such transactions” coupled with the failure to actually describe any of those illegal transactions, Paragraph 10 effectively authorizes the seizure of any document with any name on it. This is enormously overbroad. The Government simply did not establish probable cause as to every single document with any name on it related to any transaction of Kayla.

The Kayla Warrant’s other paragraphs fare no better, particularly in light of the Kayla Warrant’s failure to specify the criminal conduct at issue. As written, the searching officers are permitted to seize effectively any business record, regardless of its relation to any crime.¹¹ Such “conferral of . . . unfettered discretion on the executing officers, *particularly in light of the [warrant’s] independent failure to identify any crime under investigation*” has justified suppressing warrants before. *Wey*, 256 F. Supp. 3d at 387 (emphasis added); *see also Rosa*, 626 F.3d at 62 (search warrant failed “to link the items to be searched searched and seized to the suspected criminal activity” and “thereby lacked meaningful parameters on an otherwise limitless search”).

Even assuming certain of the Kayla Warrant’s paragraphs could be found to be sufficiently rooted in probable cause – and they cannot – the sweeping nature of the other paragraphs invalidate the Kayla Warrant as overbroad. In *Zemlyansky*, the Southern District of New York suppressed evidence seized from the Tri-State Billing office pursuant to a warrant

¹¹ See Paragraph 1 (authorizing seizure of items, including but not limited to, “[r]ecords, documents and materials regarding the identity of the corporate customers of Kayla”); Paragraph 2 (authorizing seizure of items, including but not limited to “[r]ecords, documents and materials that memorialize financial transactions between Kayla and its customers”); Paragraph 4 (authorizing seizure of items, including but not limited to, “financial transactions between Kayla and the bank or banks at which Kayla holds accounts”); Paragraph 5 (authorizing seizure of CTRs or “similar reports”); Paragraph 6 (authorizing seizure of “[a]ll logs or lists” referencing CTRs or “similar reports”); Paragraph 7 (authorizing seizure of “records, documents and materials that contain data used to prepare” CTRs (without providing any parameters on what data may be used in preparing such CTRs)); Paragraph 8 (authorizing seizure of “[r]ecords, documents or materials regarding regulatory and/or legal requirements for conducting business as a financial institution); and Paragraph 9 (authorizing seizure of “[c]orrespondence between representatives of Kayla and the government or any third party regarding reporting and filing requirements”). Siegal Aff., Ex. 2 at Att. A.

based on an affidavit that attested that some members of the alleged scheme established companies to handle paperwork and billing disputes. 945 F. Supp. 2d at 450-51. Although the affidavit provided probable cause for the search and seizure of materials relating to five particular clinics, the court held that the Government failed to establish probable cause to search and seize “*all* patient care records, bank account information, and patient information” and held the warrant to be overbroad. *Id.* at 465. In characterizing the warrant as a “prohibited general warrant,” the court explained:

Together, the Tri-State warrant authorized the officers to search for and seize almost everything that one could expect to find at a billing office: any cash or checks, any document that might be considered to be some sort of “financial instrument,” all patient records and everything else related to patient records, and all bank information. In addition to the physical evidence, the warrant authorized the unlimited search and seizure of all computers and thumb drives, as well as virtually anything electronic and anything related to the use or operation of those electronics. [I]t conferred on the searching officers discretion to seize virtually everything short of any diaries, clothing, and love letters that employees may have brought to work.

Id. at 459; *see also George*, 975 F.2d at 75 (holding warrant insufficiently particular on account of its “broad authorization to search for ‘any other evidence relating to the commission of a crime’”).

Of course, here, love letter and diaries *would* be arguably covered by Paragraph 10 if they “regarded” Kayla’s employees. Because the Kayla Warrant described overly broad categories without reference to any particular crime, it authorized the wholesale search and seizure of Kayla’s premises without the requisite showing of probable cause to do so. *See Cohan*, 628 F. Supp. 2d at 361. Such a search is impermissible under the Fourth Amendment.

II.

THE SNEDEKER AFFIDAVIT WAS MATERIALLY MISLEADING

In addition to the arguments set forth above, another basis to suppress the fruits of the Kayla Warrant is that the Magistrate Judge was misled into issuing it. The Snedeker Affidavit, on which the Kayla Warrant was issued, contained several materially misleading assertions that Agent Snedeker knew, or recklessly failed to know, were misleading when he made them. Taken as a whole, those assertions wove a fundamentally misleading picture of Kayla's operations in order to justify a broad sweep of John's business. Had Magistrate Judge Wall known the full picture, he very likely would not have issued the Kayla Warrant. At a minimum, the material omissions and misleading passages of the Snedeker Affidavit warrant holding a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978), to determine whether sufficient probable cause actually existed to support the issuance of the Kayla Warrant.

A defendant may "challenge the truthfulness or factual statements made" in an affidavit supporting a search warrant application, "and thereby undermine the validity of the warrant and the resulting search and seizure." *United States v. Mandell*, 752 F.3d 544, 551-52 (2d Cir. 2014) (citing *Franks*, 438 U.S. at 155-56); *see also Scully*, 108 F. Supp. 3d at 96 (same). As the Supreme Court explained in *Franks*:

[W]here the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

438 U.S. at 155-56.

Here, the IRS's justification for the Kayla Warrant appeared to be that Kayla's employees systematically assisted "many customers" in intentionally evading CTR filing requirements and failed to file CTR to account for transactions that amount to tens of millions of dollars. It did so

in an effort to cast Kayla as a business poisoned by illegality, and thus to justify a very broad, overly intrusive warrant. Among other things, the Snedeker Affidavit mischaracterized legitimate activities and transactions as improper, omitted to mention recorded statements that tended to exculpate Kayla’s owner (John), and touted misleading statistics to suggest broad patterns of illegality. Had the Snedeker Affidavit not contained these flawed passages and omissions, the Magistrate Judge would have received a substantially different picture of John’s business, and likely would not have approved the Kayla Warrant.

A. Agent Snedeker’s General Mischaracterization of Kayla

The Snedeker Affidavit unfairly sought to stigmatize Kayla for legitimate, legal business activity, and by improperly arguing for guilt by association of it with unrelated parties. First, it suggested that any corporate customer that used Kayla did so to evade reporting requirements. Siegal Aff., Ex. 1 at ¶ 9 (“Kayla’s customers choose to pay the *extraneous* two to three percent fee rather than cash the checks *through their respective banks at no charge in order to conceal the receipt of the income, and evade having CTRs filed on the transaction.*”) (emphasis added). Agent Snedeker stated that “Kayla primarily services customers in the construction industry,” and that within the construction industry, “Kayla is known … for *routinely assisting customers to evade income and payroll taxes.*” *Id.* at ¶¶ 8, 12. Later, Agent Snedeker said that “Kayla engaged in approximately \$97 million in cash transactions in 2011,” but “only filed \$24 million in CTRs,” indicating that more than \$73 million in transactions that year, or over \$200,000 per day, were in denominations of \$10,000 or less.” *Id.* at ¶ 30. If Kayla serviced mostly corporate construction companies, and those companies deposited large sums at Kayla, then the implication here was that Kayla must have failed to file CTRs on some substantial portion of the remaining \$73 million, and was doing so intentionally.

Taken together, those assertions are misleading at best. As a general matter, there is nothing illegal about using (or operating) a check-cashing company, and it is simply untrue to suggest that every company (or even most) that uses a check casher does so to evade paying taxes. In reality, corporate customers often use check-cashing companies even if it means paying a two to three percent service charge (which every check-cashing institution legally charges), for perfectly legitimate, legal business reasons, including because check cashers provide funds immediately. Many banks, by contrast, require customers to wait at least one and as many as several full business days for checks to clear (the Snedeker Affidavit admitted this point, but nevertheless suggested that using check cashers was done only for nefarious reasons). For customers in the construction industry – and even Agent Snedeker acknowledged that such customers constituted a significant portion of Kayla’s corporate customer base – it is often critical, for legitimate business purposes, to have funds immediately to pay workers and subcontractors.¹² Thus the fee paid by such customers to Kayla cannot fairly be described as “extraneous,” nor as proof of inherent criminality in Kayla’s operation.

Moreover, the Government’s insinuation that Kayla failed to file CTRs on approximately \$73 million in transactions is simply a baseless assertion. With some overly simplistic math, Agent Snedeker divided \$73 million by 365 – the numbers of days in the year – and argued that “\$200,000 per day” suggests that a large portion of Kayla’s business required CTRs that were going unfiled. What Agent Snedeker conveniently omitted to mention as part of his “analysis” is that (a) the business has *six (6) storefronts*, which means that if those storefronts each averaged

¹² Check-cashing institutions also provide “important and vital” services to the communities they service. *See, e.g.*, 3 N.Y.C.R.R. § 400.14 (“The legislature hereby finds and declares that check cashers provide important and vital services to New York citizens; that the business of check cashers shall be supervised and regulated through the [Banking] Department in such a manner as to maintain consumer confidence in such business and protect the public interest; that the licensing of check cashers shall be determined in accordance with the needs of the communities they are to serve; and that it is in the public interest to promote the stability of the check cashing business for the purpose of meeting the needs of the communities that are served by check cashers.”)

more than three customers cashing checks each day, the average such transaction would be below \$10,000 in every instance. Moreover, the customer volume of the business was in fact much greater than that. On average, there were in excess of *400 transactions* per day.¹³ Since the law requires the filing of a CTR only when a customer receives *more than* \$10,000, the fact that only approximately 25 percent of Kayla's business in 2011 generated a CTR is wholly unsurprising, and Agent Snedeker's misleading "statistical analysis" amounts to nothing more than baseless speculation. Certainly it was no proof of a pattern of wrongdoing by the Kayla entities.

In fact, it is not only entirely plausible, but extremely likely, that Kayla would not have been required to file CTRs on about \$73 million in transactions in 2011. Assuming Kayla was used for 40,000 commercial transactions in a given year (which is average for Kayla) and a commercial customer's average daily deposit was around \$2,400, then Kayla would not have been required to file CTRs for more than \$80 million in transactions.

Given Agent Snedeker's experience, training, and purported knowledge of the check-cashing industry, he should have known that CTRs would not be required for a significant majority of ordinary check-cashing transactions, and that even large construction companies cash checks in small denominations. Instead, he carelessly and baselessly insinuated that Kayla was pivotal in helping bad actors avoid paying taxes on tens of millions of dollars, when he knew or should have known that his "statistics" provided no basis for that unsupported assertion.

¹³ The statement that one third of Kayla's 2012 cash transactions resulted in CTRs being filed is of no moment for the same reasons.

B. Agent Snedeker Omitted Recorded Information Tending to Exculpate the Boss (*i.e.*, John)

The IRS relies heavily on the efforts of a cooperating witness (the CW) – a man who pled guilty to tax fraud about a year before he began cooperating with the Government – to buttress its theory that “Kayla is known . . . for routinely assisting customers to evade income and payroll taxes by circumventing the federal currency reporting requirements” and that “employees of Kayla instruct many of their customers how to intentionally evade CTR filing requirements.” Siegal Aff., Ex. 1 at ¶ 12. The Affidavit, however, omitted important information obtained during the CW’s undercover recordings that would tend to show that the improper actions of two of Kayla’s salespeople (Mr. H., a salesman for Kayla, and Mr. C., who worked for Mr. H.), were not approved or condoned by the “boss,” – *i.e.*, John.

In describing his investigation, Agent Snedeker paraphrased or quoted selected snippets of undercover footage involving the CW and either Mr. H. or Mr. C. from 2012. Left out of the Snedeker Affidavit entirely was any description of recorded evidence in the Government’s possession suggesting that Kayla management (including John) did not tolerate structuring. On three separate occasions, either Mr. C. or Mr. H. is caught on tape alerting the CW that they would not be able to help the CW avoid the filing of a CTR if their boss was present. *See Siegal, Aff.* ¶¶ 9, 10, 11. On August 30, 2012, for example, Mr. H. told the CW that “I can do it for you every once in a while, but sometimes when my boss is here, you know. . .” *Id.* ¶ 9. Similarly, on September 12, 2012, Mr. C. informed the CW that he could not structure his transactions when “the boss” was around: “Yeah, it is just different when the uh, when the boss is in. It gets tough . . . he wants things signed [and] he wants things done the right way. I don’t do things the right way, you know what I mean?” *Id.* ¶ 10. And on September 25, 2012, Mr. C. told the CW he

could help him structure his transactions, because “when my boss is not in, *not* a problem.” *Id.* ¶ 11 (emphasis added).

C. Additional Omissions and Misleading Assertions

Agent Snedeker also alleged that at some point between 2006 and 2012, Kayla failed to file CTRs for several other customers who were now the subject of the IRS’s investigation. However, for four of the seven individual customers mentioned, Agent Snedeker did not aver that anyone at Kayla told them to structure or instructed them on how to avoid reporting requirements, nor aver that those individuals structured at all. He simply attested that these individuals were alleged to have committed tax fraud, and that they used Kayla’s or other check casher’s services. *See Siegal Aff., Ex. 1 at ¶¶ 24-27.* In this way, Agent Snedeker misleadingly implied a connection between Kayla and those customers’ own tax evasion for which he (apparently) had no evidence. This is plainly a guilt-by-association assertion, and nothing more.

In fact – and what Agent Snedeker leaves out – John Drago and Kayla *did not help these individuals evade reporting requirements.* The Snedeker Affidavit omitted to inform the Court that Kayla actually filed numerous CTRs on those customers’ transactions¹⁴ (as well as thousands of other transactions), despite the fact that Agent Snedeker had access to that fact at the time he swore his Affidavit.

Most notably, the Snedeker Affidavit misstated Kayla’s reporting of customer “J.G.’s” transactions. In fact, Kayla filed *60 CTRs for J.G.’s transactions* between August 2010 and December 2012, *covering more than \$1.14 million* – not (as Agent Snedeker incorrectly

¹⁴ To the extent suspected money launderers or tax evaders seek to fly under the radar without Government detection, the fact that Kayla filed CTRs on these customers would tend to have frustrated that purpose. *See United States v. Mazza-Alaluf*, 607 F. Supp. 2d 484, 493 (S.D.N.Y. 2009) (stating that the Bank Secrecy Act, which includes the Currency and Foreign Transactions Reporting Act, “was intended to provide an investigative tool for criminal, tax, and regulatory matters.”). By filing CTRs, Kayla alerted the Government to these individuals’ names and transactions, and therefore any suggestion that Kayla helped these individuals avoid detection lacks merit.

asserted), on “less than \$711,000.” (Despite acknowledging that J.G. owned and operated two companies, Agent Snedeker omitted from his math the fact Kayla filed CTRs on almost \$450,000 worth of transactions for one of those companies). Siegal Aff., Ex. 6.

Similarly, Kayla also filed CTRs on James G. (38 CTRs covering about \$1.8 million in transactions for the 2010 and 2011 period); Kevin C. (at least 36 CTRs covering over \$600,000 for just 2008 and 2009; 2006 and 2007 data is not available); Thomas B. (eight CTRs covering about \$102,000 in transactions from August 2010 to December 2012); and Mark H. (five CTRs covering about \$120,000 in 2010).¹⁵ All of this was omitted from the Snedeker Affidavit.

Agent Snedeker also misleadingly stated that Kayla failed to file Suspicious Activity Reports (“SARs”) on J.G.’s transactions. While it may be true that SARs were not filed, that is of no moment at all, because *no requirement exists* for check-cashing companies to file SARs. See MSBs Subject to SAR Requirement, available at <https://www.fincen.gov/msbs-subject-sar-requirement> (“[t]he SAR requirement does not apply to the following types of [money services businesses]: Check casher...”); see also 31 C.F.R 1022.320(1) (“Every money services business described in § 1010.100(ff)(1), (3), (4), (5), (6), and (7) ... shall file with the Treasury Department... a report of any suspicious transaction...”); 31 CFR 1010.100(ff)(2) (defining “check casher”). Again, taken in context, the assertion that Kayla did not file SARs was undoubtedly inserted to unfairly paint Kayla as a lawbreaking business. The failure to note, in that context, that no such requirement exists is another example of a critical piece of information that the Magistrate Judge did not have when he decided to approve the proposed warrant – a warrant that likely would otherwise not have appeared justified.

¹⁵ To respect their privacy, we are not listing the full names of these individuals in a publicly filed document, but we are happy to provide this information to the Court and the Government.

Taken together, the omissions and misleading statements in Agent Snedeker's Affidavit carelessly and recklessly (at least) had the effect of misleading Magistrate Judge Wall into concluding that probable cause for a search warrant for Kayla was justified. Stripped of its misleading allegations, what remains of the Snedeker Affidavit simply does not support a finding of probable cause to search Kayla's premises. *See Franks*, 438 U.S. at 156 (where the "allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit."). On the whole, the false and misleading statements detailed above suggest at least recklessness on the part of the IRS.

Thus, the Court should, at the least, hold a *Franks* hearing to determine whether Magistrate Judge Wall would have issued the warrant for Kayla but for the misleading statements and omissions in the application. *See, e.g., United States v. Butt*, No. 18-CR-00087 (NSR), 2018 U.S. Dist. LEXIS 169729, at *10-11 (S.D.N.Y. Oct. 1, 2018) (granting *Franks* hearing where affidavit submitted in support of search warrant contained allegedly false statements and those statements were material to the probable cause determination); *United States v. Westover*, 812 F. Supp. 38, 40 (D. Vt. 1992) (granting *Franks* hearing where, without the allegedly false statements, there were insufficient facts to justify a finding of probable cause); *United States v. McMurtrey*, 704 F.3d 502, 510 (7th Cir. 2013) (*Franks* hearing was warranted where the affidavit in support of the search warrant conflicted with the affidavit and account of another law enforcement official); *United States v. Johns*, 851 F.2d 1131, 1133-34 (9th Cir.

1988) (remanding for a *Franks* hearing where the defendant alleged that portions of the affidavit in support of the search warrant could not have been true).

III.

THE GOVERNMENT'S FIVE-YEAR RETENTION OF NEARLY EVERY FILE SEIZED CONSTITUTES AN UNREASONABLE SEARCH AND SEIZURE IN VIOLATION OF JOHN'S FOURTH AMENDMENT RIGHTS

The August 2013 search of Kayla resulted in the seizure of more than 20 boxes of hard copy documents and mirror images of 11 computers. Since then, more than five years later, the Government continues to maintain possession of every document seized (including all the hard-copy originals and full images of the original electronic storage devices). *See Siegal Aff.* ¶ 12. This retention of all computers and electronics, as well as virtually all of Kayla's records, presents a separate violation of John's constitutional rights that should be remedied by suppressing the fruits of the search. The Government should also be precluded from conducting any further review of Kayla's computers at this point, pursuant to Second Circuit precedent.

As a general matter, where a warrant authorizes a search through vast quantities of computer files, the Fourth Amendment's particularity requirement becomes even more important. *See Galpin*, 720 F.3d at 446; *Ganias I*, 755 F.3d at 135; *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017); *Cioffi*, 668 F. Supp. 2d at 391. Indeed, courts have increasingly emphasized the need for "greater vigilance" by judicial officers to ensure that the process of identifying data subject to seizure does not become "a vehicle for the government to gain access to data which it has no probable cause to collect." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010).

As the Second Circuit has stated, it is constitutionally unreasonable for the Government to seize and indefinitely retain every file on a defendant's computer for use in future criminal investigations. *See Ganias I*, 755 F.3d at 127-28. Rather, the Government must review the

relevant materials and return those not covered by the warrant in a reasonable time. *See United States v. Alston*, No. 15 Cr. 435 (CM), 2016 U.S. Dist. LEXIS 63776 at *8 (S.D.N.Y. Apr. 29, 2016); *United States v. Soliman*, No. 06-CR-236, 2008 U.S. Dist. LEXIS 87304, at *1-2 (W.D.N.Y. Oct. 29, 2008); *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177 (stating that the government may only retain material seized from electronic systems if the materials were specified in the warrant).

Though courts have recognized the need for the Government to conduct off-site searches of a computer and to allow for mirroring of a computer's hard drive, the Fourth Amendment requires the Government to complete its review – *i.e.*, execute the search warrant – within a “reasonable” period of time. *See United States v. Metter*, 860 F. Supp. 2d 205, 211-12 (E.D.N.Y. 2012)¹⁶. Indeed, the Government should not be “permitted to return to the proverbial well months or years after the relevant Warrant has expired to make another sweep for relevant evidence” *Wey*, 256 F. Supp. 3d at 406; *see also Metter*, 860 F. Supp. 2d at 216 (15-month delay in reviewing hard drive images held unconstitutional); *United States v. Debbi*, 244 F. Supp. 2d 235, 238 (S.D.N.Y. 2003) (eight-month delay in reviewing search material held to violate the Fourth Amendment).

Once the Government completes its review, it must return all non-responsive information which “[i]t [had] no probable cause to collect.” *See, e.g., Comprehensive Drug Testing*, 621 F.3d at 1177; *see also United States v. Tamura*, 694 F.2d 591, 596-97 (9th Cir. 1982) (retention of documents not described in warrant for six months after locating relevant documents was

¹⁶ The Government’s internal policy guidance on searches and seizures provides the same guidance – *i.e.*, “[t]he Fourth Amendment does require that forensic analysis of a computer be conducted within a reasonable time.” *See Exec. Office for U.S. Attorneys, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 77 (2009), available at <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>, DOJ Manual at 92.

“unreasonable and therefore unconstitutional”); *Ganias I*, 755 F.3d 125 at 127-38 (describing retention of non-responsive documents for year and a half as “clearly violating” defendant’s Fourth Amendment rights).

As this District has said, allowing the Government to shirk its Fourth Amendment responsibilities by indefinitely retaining materials would cause “the Fourth Amendment [to] lose all force and meaning in the digital era[,]” where “citizens [would] have no recourse as to the unlawful seizure of information that falls outside the scope of a search warrant and its subsequent dissemination.” *Metter*, 860 F. Supp. 2d at 216.

Here, the Government’s retention for more than five years of the entirety of documents and electronic images seized from Kayla in August 2013 (while purging nothing), even in the face of oral and written requests for their return, was and continues to be, a flagrant disregard of the Fourth Amendment. *See, e.g., Metter*, 860 F. Supp. 2d at 215-17. The Government has not explained what it has been doing over the last five years, nor why it took so long to bring charges on what appears to be information from on or before the August 2013 search.

Notwithstanding counsel’s efforts, it is still unclear at this stage if the Government retained the material to revisit it five years later to bring the instant charges, or whether the Government set the material aside and never looked at it at all, or if it did review it, when that review was completed; how responsive information was identified (if at all) and separated from the non-responsive information; what the Government did (if anything) to purge itself of the non-responsive data; or whether it went “back to the well” recently, and re-accessed information previously deemed by it to be unresponsive to the original warrant.

Whether the Government culled the materials and segregated the responsive from the non-responsive, however, is at some level of no moment, if the Government continued to retain

all the materials, because in doing so, its continued retention, in and of itself, “becomes the equivalent of an unlawful general warrant.” *See Ganias II*, 824 F.3d at 232 (Chin, J. dissenting). If the Government has not looked at the computer images in the five years during which it has possessed them, then it should be precluded from doing so now.

IV.

THE SEARCH AND SEIZURE OF JOHN’S CELL PHONE WERE UNCONSTITUTIONAL, AND ITS EVIDENCE MUST BE SUPPRESSED

The Government again violated John’s Fourth Amendment rights by unlawfully seizing his cell phone on August 1, 2018, and thereafter by searching it pursuant to an unconstitutional and facially invalid “general warrant.”

A. The Government Unlawfully Seized John’s Cell Phone

After John’s arrest, an IRS agent handed John his cell phone to call his attorney and then unlawfully seized it, stating that they had the authority to do so because it was “on his person.” Drago Aff. ¶ 7. Though Agent McCue claims that John “consented” to turning over his cell phone, *see Siegal Aff. Ex. 4 at ¶ 6*, John was misled when he was told that the IRS already had a warrant (which did not then exist) to seize his phone. Drago Aff. ¶ 7. Because the search-incident-to-arrest exception to the warrant requirement does not apply under such circumstances, and because any “consent” by John to hand over the phone was not voluntary under the circumstances, any “evidence” obtained from John’s phone must be suppressed.

The Fourth Amendment’s warrant requirement is “critical to safeguarding a person’s privacy interests from unreasonable government intrusion.” *United States v. DiMarco*, No. 12 CR 205 (RPP), 2013 U.S. Dist. LEXIS 16279, at *20 (S.D.N.Y. Feb. 5, 2013); *see McDonald v. United States*, 335 U.S. 451, 455-56 (1948) (“Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done . . .

[because t]he right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and arrest of criminals.”). Because of the importance of a person’s privacy interests, the Supreme Court has consistently held that searches conducted without a warrant are “per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions.” *Katz v. United States*, 389 U.S. 347, 357 (1967) (footnote omitted)

Indeed, “the general constitutional requirement that a search warrant be obtained ‘is not lightly to be dispensed with,’ and the proper extent of such searches must be limited by the rationale that permits such warrantless intrusions. *United States v. Marotta*, 326 F. Supp. 377, 382 (S.D.N.Y. 1971) (*citing Chimel v. California*, 395 U.S. 752, 762-63 (1969)). The scope of the search incident to arrest exception must be commensurate with its purposes: “protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy.” *Gant*, 556 U.S. at 339; *see also United States v. Lartey*, 716 F.2d 955, 965-66 (2d Cir. 1983); *United States v. Marotta*, 326 F. Supp. 377, 382 (S.D.N.Y. 1971). In such circumstances, an officer may search the arrestee’s person and the area within his immediate control, which means “the area from within which he might gain possession of a weapon or destructible evidence.” *Chimel*, 395 U.S. at 763. It does not, however, authorize the search of rooms other than that in which the arrest occurs. *See id.* at 762-63.

In a case similar to this one from the Southern District of New York, *United States v. Marotta*, the defendant moved to suppress evidence seized pursuant to the incident to arrest exception where the defendant was arrested in the entrance of his apartment and a firearm was seized from a bedroom down the hall. 326 F. Supp. at 383-84. The court noted that, though the agents could permissibly have searched the defendant’s person and seized any evidence or

weapon found on him, or the area where the arrest was made and from within which the defendant may have been able to obtain or destroy evidence, the agent could not ask the defendant where other firearms were kept and then search a room down the hall and separate from the area in which the arrest occurred. *Id.*

Like the defendant in *Marotta*, John was arrested in a different area than the room ultimately searched. Drago Aff. ¶¶ 6-7. Once John was handcuffed, he was escorted from the main level of his home to the upstairs area by an agent, who, upon entering the bedroom, walked to the other side of the room, picked up the phone from a nightstand, and handed it to John. *Id.* ¶ 7. Here, too, the agent seized evidence in a place distinct from the place of arrest. There simply was no way that John could have accessed his phone but for the agent's bringing him to it.

Moreover, seizing evidence from John's bedroom does not comport with the rationale underlying the search incident exception. A phone does not threaten officer safety the way a gun or a knife would. *See Marotta*, 326 F. Supp. at 382. Nor could the officer have been motivated by a desire to preserve evidence that could be concealed or destroyed; had this been the case, he would not have put the phone into John's possession in the first place. Directing John to his phone under the guise of allowing him to call his attorney, only to use it as a pretext to seize it thereafter, is unconstitutional. Accordingly, the seizure of John's cell phone cannot be justified under the search incident to arrest exception.

Further, under the circumstances, given that John was in custody and was told by the agents, falsely, that the law permitted the agents to seize the phone because it was "on him," and (also falsely) that the agents already had a warrant for it, no "consent" to turn it over could have been voluntary. *Bumper v. Carolina*, 391 U.S. 543, 548 (1968) ("The issue thus presented is whether a search can be justified as lawful on the basis of consent when that 'consent' has been

given only after the official conducting the search has asserted that he possesses a warrant. We hold that there can be no consent under such circumstances.”); *Breitbard v. Mitchell*, 390 F. Supp. 2d 237, 248 (E.D.N.Y. 2005) (“[P]laintiff’s consent was conditioned on the police having a warrant, which they did not . . .”)

B. The Phone Warrant Is a facially Invalid “General” Warrant

As with the Kayla Warrant, the Phone Warrant too is insufficiently particularized and overbroad. It therefore violates the Fourth Amendment, and any fruits seized pursuant to it must be suppressed.

1. The Phone Warrant Does Not Describe with Particularity the Items to Be Seized

The Phone Warrant is invalid on its face because it fails to describe with particularity the items to be seized. As a critical preliminary matter, the Phone Warrant actually authorizes the search of *someone else’s Apple iPhone* (see Siegal Aff. Ex. 5 at 3 (Attachment A to the Phone Warrant)) – not John’s Samsung Galaxy S9 – and thus the Government therefore does not even currently have a warrant authorizing it to search John’s Samsung phone.

In addition, Attachment B to the Phone Warrant enumerates eight broad categories of records that could exist on any cell phone, and then grants the Government apparent authority to search the phone in its entirety for those records. Among the all-encompassing categories listed on Attachment B is authority to search for “contextual information” necessary to shed light on the other impermissibly broad categories of information, as infinitely malleable an authorization as ever there was one. *Id.* at Att. B, ¶ 8. The Phone Warrant does not provide any parameters for what can be searched – by subject matter, time frame, or otherwise – and instead opens John’s cell phone to the type of “wide-ranging exploratory search[]” that courts routinely deem unconstitutional. *See, e.g., Garrison*, 480 U.S. at 84.

When a warrant authorizes the search for electronic information, “the particularity requirement assumes even greater importance.” *Galpin*, 720 F.3d at 44. That is because electronic media has the “ability to store and intermingle a huge array of one’s personal papers in a single place,” which thereby “increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs” absent a narrowly tailored warrant. *Rosa*, 626 F.3d at 62 (2d Cir. 2010) (citation omitted); *see also Ganias II*, 824 F.3d at 231 (Chin, J., dissenting) (nothing that “[v]irtually the entirety of a person’s life may be captured as data” on a smartphone or computer). Here, the particularity requirement was simply ignored. Indeed, the Phone Warrant suffers from several deficiencies, each of which render it unconstitutionally overbroad.

For instance, Attachment B lists items that are wholly unrelated to criminal activity and therefore do not “describe with adequate particularity the items to be seized by their relation to designated crimes.” *Galpin*, 720 F.3d at 450 (internal quotation marks omitted). Paragraph 6 of Attachment B allows for the search for “[e]vidence of the times the MOBILE DEVICE was used,” irrespective of any limiting factor pinning that to any alleged wrongdoing – *e.g.*, a time frame within which alleged misconduct occurred (which is wholly absent from not just the Phone Warrant, but also the supporting McCue Affidavit, as discussed more fully below). Likewise, Paragraph 7 of Attachment B allows for the search and seizure of passwords generally – *e.g.*, not for a particular application that John is alleged to have used in furtherance of some purported crime, but rather any password, for any app or website or function or account!

Even where Attachment B references statutory provisions, *see Siegal Aff.*, Ex. 5 at ¶ 8, mere references to statutes do not cure the Phone Warrant’s failure to indicate which specific acts of wrongdoing are being investigated. *See Galpin*, 720 F.3d at 445 n.5 (“Mindful that the purpose of this requirement to minimize the discretion of the executing officer, other Circuits

have held that even warrants that identify catchall statutory provisions, like the mail fraud or conspiracy statutes, may fail to comply with this aspect of the particularization requirement”); *United States v. Maxwell*, 920 F.2d 1028, 1033 (D.C. Cir. 1990) (“References to broad statutes realistically constitute no limitation at all on the scope of an otherwise overbroad warrant and therefore cannot save it.”); *United States v. Roche*, 614 F.2d 6, 8 (1st Cir. 1980) (footnote omitted) (“[S]ection 1341 makes illegal all frauds that utilize the mails; limitation by so broad a statute is no limitation at all.” (footnote omitted)); *Vilar*, 2007 U.S. Dist. LEXIS 26993, at *68 (concluding that “oblique reference” in warrant rider to “participants in the fraud schemes” could not cure warrant’s failure to “indicate what specific acts of wrongdoing are being investigated”).

Here, Attachment B references “violations of Title 18, United States Code, Sections 371 [conspiracy], 666 [theft or bribery concerning programs receiving federal funds], 1341 [mail fraud], 1343 [wire fraud],¹⁷ 1349 [conspiracy], 1956 [money laundering], and 1957 [monetary transactions with proceeds of unlawful activity] – that is, several among the broadest, most unilluminating sections of the U.S. Code. Siegal Aff. Ex. 5. Though the McCue Affidavit averred that there was probable cause to believe that the phone contained evidence of Bank Secrecy Act violations, Attachment B does not refer to Title 31 nor the Bank Secrecy Act at all. Attachment B does not provide any discernible guidance to the agents (or to the Warrant’s recipient) as to what kinds of files or information can be seized, nor does it connect any of the information sought with criminal activity. As such, no agent reviewing the Phone Warrant could reasonably determine what should and should not be seized.

¹⁷ Attachment B to the Phone Warrant is actually internally inconsistent on this point, sometimes including, and other times *not* including, 1343 in its list of offenses. Siegal Aff. Ex. 5 (Compare Attachment B first preamble paragraph to second preamble paragraph and Paragraph 8.)

Instead, this Phone Warrant would permit agents to proceed as though anything can be seized, according to their whim. Attachment B provides for the review of “*all records and information*” on the phone, including “names and telephone numbers . . . the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet Activity . . . and other electronic media.” *Id.* It then lists out eight illustrative categories of information that are included in the aforementioned “all records and information” catch-all, including amorphous categories like “evidence of . . . who used [the phone],” “[e]vidence of times the [phone] was used” and “[c]ontextual information necessary to understand the evidence described in this attachment.” *Id.* By Agent McCue’s own admission, the examination “might expose many parts of the MOBILE DEVICE to human inspection in order to determine whether it is evidence described by the warrant.” Siegal Aff. Ex. 4 at ¶ 13.

Put simply, Attachment B allows the Government to search the entire phone for information regardless of its relationship to any criminal activity. In other words, the face of the Phone Warrant would permit the Government to intrude into the most personal aspects of John’s life – including his text messages with family and friends, personal photographs, password-protected social media accounts – in “search” of anything that the Government can latch onto as a way of tying John to some wrongdoing – *any* wrongdoing. The overwhelming breadth of these search parameters alone renders the Phone Warrant insufficiently particularized. The conclusion is inexorable that the Phone Warrant impermissibly authorizes the search and seizure of any and all records on John’s cell phone – *i.e.*, that it is a general warrant.

Finally, Attachment B fails to provide a temporal limitation for the search, which also renders it overbroad. *See, e.g., Wey*, 256 F. Supp. 3d at 387 (“Finally, to the extent that lack of

temporal limitation constitutes an independent factor militating against a determination of particularity, the Warrants undisputedly fail to limit the items subject to seizure by reference to any relevant timeframe or dates of interest.”); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant “not sufficiently particular” where “[t]he government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place”); *United States v. Jacobson*, 4 F. Supp. 3d 515, 526 (E.D.N.Y. 2014) (“[A] warrant’s failure to include a temporal limitation on the things to be seized may, in certain circumstances, render a warrant insufficiently particular[.]”). Even if the McCue Affidavit was incorporated or annexed to the Phone Warrant, it similarly omitted all references to the time frame under investigation (which, as explained below, may have been a deliberate tactic to hide the fact that John was arrested for alleged conduct in the 2010-2013 period, which would have highlighted the lack of probable cause to search a cell phone that did not *exist* until approximately March 2018). In any event, because the McCue Affidavit was not annexed to the Phone Warrant, it cannot salvage the Phone Warrant’s facial deficiencies for the same reasons explained above in Section VI., *supra*.

2. The List of Items is Overbroad and Lacks Probable Cause

The Phone Warrant describes overly broad categories of information that may be seized, irrespective of their relationship to any particular crime. The Government’s failure to establish probable cause for such a broad search provides an independent basis for deeming the Phone Warrant deficient.

As explained above in Section I.B., *supra*, where a warrant permits a “fairly broad” search, the affidavit in support of the warrant must “provide[] the necessary basis for a determination of probable cause to seize items in each of those categories.” *Zemlyansky*, 945 F. Supp. 2d at 464 (internal quotation marks omitted). Here, the McCue Affidavit does not establish probable cause for the alleged crimes at all, much less for the incredibly broad

categories listed in Attachment B. Nowhere in the McCue Affidavit did she provide any details that would even *suggest* John's involvement in mail or wire fraud, money laundering activity, or theft or bribery from federal programs, much less provide the requisite level of detail to justify an all-encompassing search of John's phone. Moreover, the references to John's control of Kayla and purported failure to report payroll taxes include generic, conclusory statements that are unsupported by particular facts or details of the purported investigation into John. Siegal Aff. Ex. 4 at ¶¶ 5-7. Neither of these passing references support the broad sweep of John's phone for violations of the Bank Secrecy Act (which the Warrant itself fails to mention in any event), and certainly do not provide probable cause for the several other unrelated crimes. *See Zemlyansky*, 945 F. Supp 2d at 464-65 (suppressing evidence where Government failed to establish probable cause to search and seize all records contemplated by warrant).

3. The McCue Affidavit Was Materially Misleading

The fruits of the Phone Warrant should be suppressed because Magistrate Judge Tomlinson was misled into issuing it. The McCue Affidavit, on which the Phone Warrant was issued, contained several key omissions that Agent McCue should have known or recklessly failed to know were false and misleading. Ultimately, through vague and unsupported assertions in her sworn testimony, Agent McCue suggested that John was indicted for several crimes for which he was not actually indicted, and that his phone contained evidence of those crimes, even though his phone was a few months old at the time of the seizure and the Indictment's charges date back to, at the latest, *five years prior*.

Agent McCue generally averred that John's cell phone holds evidence of violations of the Bank Secrecy Act, as well as crimes for which he was never charged, including wire fraud, conspiracy, and money laundering. Her Affidavit is devoid of support for those statements. In fact, the majority of the McCue Affidavit concerns Agent McCue's experience and purported

knowledge of the investigation, or the nature of cell phones generally. *See Siegal Aff. Ex. 4, ¶¶ 1-3, 8-9, 11-15.* The rest of the Affidavit fails to support the issuance of the Phone Warrant.

In fact, only two paragraphs hint at actual wrongdoing, though they do not provide any basis for Agent McCue’s statements. The first reference to wrongdoing is in Paragraph 5, where Agent McCue alleged that John diverted cash income from Kayla to pay his employees – a tax offense – which is *not* referenced in the warrant. *Id.* at ¶ 5. The other reference is to John’s purported “approval” of the advancing of money to customers and cashing of post-dated checks. *Id.* at ¶ 7. There is no further support for these allegations such that a Magistrate Judge could find that probable cause existed to support a search for evidence of the Bank Secrecy Act charges, and per Attachment B, the Government does not intend to search for evidence of the tax-related offenses. The rest of the Affidavit did not even mention wrongdoing that could substantiate Agent McCue’s allegations that evidence of other crimes exist, much less explain why probable cause existed to support them or, more importantly, that evidence of such crimes would be found on his Cell Phone. For instance, there were no allegations of wire fraud that would support an allegation of wire fraud or conspiracy to commit wire fraud. The same goes for the money laundering charges.

Instead of providing actual support for her allegations, Agent McCue mentioned John’s arrest in August 2018 to imply that John was arrested for various offenses for which he was not. For instance, Agent McCue averred that based on her investigation and John’s alleged statements during the arrest, “it is clear” that John’s electronic communications will “substantiate his *involvement to defraud the U.S. Government*” and the wire fraud, conspiracy, money laundering, and Bank Secrecy Act violations. *Id.* at ¶ 10 (emphasis added).

Agent McCue omitted several key facts that undercut such a finding, however. Critically, she left out that John was arrested *only* for Bank Secrecy Act violations and tax-related offenses – not for mail fraud, racketeering, or money laundering, or for defrauding the U.S. Government. She also failed to mention that all these violations are alleged to have occurred somewhere in the January 2010 to October 2013 period, *many years before* August 2018 when John was arrested. And, despite her research and consulting Samsung’s technical specifications, Agent McCue omitted to reveal that the Samsung Galaxy S9 was released to the public in March 2018 – almost five years after the latest date covered by the charges in the Indictment. Thus, the claim by the Government that the Cell Phone was likely, in the slightest, to contain evidence of crimes for which probable cause could be established was effectively non-existent. Yet Agent McCue glossed right over all that, leaving it all out, and proceeded to seek this warrant.

When the McCue Affidavit is viewed in light of these additional critical facts, no conclusion can realistically be reached other than that the Affidavit recklessly (at the least) misled Magistrate Judge Tomlinson into issuing a search warrant where no conceivable probable cause could have been shown. The Court should strike this warrant altogether based on the misleading statements in this application, or at least it should hold a hearing pursuant to *Franks* to determine whether sufficient probable cause existed to support the issuance of the Phone Warrant, once the mischaracterizations are stripped away. *See, e.g., Butt*, 2018 U.S. Dist. LEXIS 169729, at *10-11; *United States v. Rajaratnam*, No. 09-CR-1184 (RJH), 2010 U.S. Dist. LEXIS 82390, at *6-7 (S.D.N.Y. Aug. 12, 2010) (granting *Franks* hearing where defendant made a substantial preliminary showing that the government recklessly or knowingly omitted several key facts from its warrant application).

V.

CERTAIN CHARGES SHOULD BE PARTICULARIZED OR DISMISSED

A. Count One Is Duplicitous

Because Count One is improperly “duplicitous,” the Government cannot proceed with the Indictment as is.¹⁸ “An indictment is impermissibly duplicitous where: 1) it combines two or more distinct crimes into one count in contravention of Fed. R. Crim. P. 8(a)’s requirement that there be ‘a separate count for each offense,’ and 2) the defendant is prejudiced thereby.” *United States v. Sturdivant*, 244 F.3d 71, 75 (2d. Cir. 2001). In determining whether a defendant was prejudiced by a duplicitous indictment, the Second Circuit has considered whether:

- (a) a general verdict of guilty could conceal a finding of guilty as to one crime and a finding of not guilty as to another;
- (b) jurors were unanimous as to any one of the crimes charged;
- (c) the defendant had adequate notice of the charges;
- (d) the Court had a basis for appropriate sentencing; and
- (e) the defendant is protected against double jeopardy in subsequent prosecutions.

Id. (internal quotations omitted).

Count One charges John with “knowingly and willfully caus[ing] and attempt[ing] to cause ... the Kayla Companies, to fail to file *one or more [CTR}s* . . . as part of a pattern of illegal activity...” on or about and between January 1, 2010 and October 31, 2013. Indictment ¶ 17. From the bare details of the Indictment, it appears that John is alleged to have caused Kayla to fail to file more than one CTR, though it is not clear how many CTRs are alleged not to

¹⁸ John reserves the right to move with respect to Count Three on the grounds of duplicity. To date, the Government has not identified the customers for whom John is alleged to have structured transactions. This issue is the subject of the request for a bill of particulars in Section VI., *infra*. Until the request for a bill of particulars is granted, John is not in a position to discern whether Count Three is duplicitous because the Government has not provided details sufficient to know whether that count refers to a single customer or multiple customers.

have been filed properly (or on whose behalf they should have been filed, the dates of the transactions that are at issue, or the amounts of the transactions).¹⁹ The jury, therefore, will be required to determine whether the Government has proven John’s involvement with respect to multiple failures to file CTRs. As charged, it will be impossible to discern, for instance, whether a verdict of guilty on Count One means that the jury unanimously determined that John caused Kayla to fail to file a CTR for Transaction “A” as opposed to Transactions “B” or “C,” or some combination or subset of the three.

This fundamental ambiguousness of the charges violates John’s constitutional right to be proven guilty beyond a reasonable doubt on a unanimous vote of the jury. *See, e.g., United States v. Murray*, 618 F.2d 892, 896 (2d Cir. 1980) (“Moreover, a guilty verdict on a duplicitous indictment does not indicate whether the jury found defendant guilty without having reached a unanimous verdict on the commission of a particular offense.”); *United States v. Crisci*, 273 F.3d 235, 238 (2d Cir. 2001) (“The vice of a duplicitous charge is that it risks to impair ‘a defendant’s right[] . . . to a unanimous verdict . . .’”). It also makes it impossible for the Court to determine whether any alleged failures to file involved more than \$100,000 in a 12-month period, which would trigger 31 U.S.C. § 5322(b), the sentence enhancement provision that the Government has alleged is applicable here.

If the Court finds that the Government has alleged duplicitous counts – and it should, based solely on the general language of the Indictment that suggests multiple CTR filings are at issue under Count One – then it should (1) require that the Government separate into different counts each alleged failure to file a CTR, and (2) as more fully discussed in Section VI., *infra*, specify in a bill of particulars the date(s), amount of the transaction(s) at issue, and the

¹⁹ As discussed further in Section VI., *infra*, the Indictment fails to specify other information that would put John on notice of the claims against him.

customer(s) on whose behalf the CTR should have been filed. *See United States v. Wilson*, No. 95 Cr. 668 (LMM), 1997 U.S. Dist. LEXIS 125, at *11 (S.D.N.Y. Jan. 8, 1997); *United States v. Willis*, 475 F. Supp. 2d 269, 274 (W.D.N.Y. 2007) (“Although a bill of particulars will not itself cure a duplicitous indictment . . . it is appropriate to order a bill of particulars “where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused.”) (internal citations omitted). If the Government does not (or cannot) provide an adequate bill of particulars for Count One, then the Court should dismiss it. *See United States v. Kearney*, 451 F. Supp. 33, 38 (S.D.N.Y. 1978) (dismissing a duplicitous indictment that “wholly failed to ‘fully, directly and expressly, without uncertainty or ambiguity, set forth all the elements necessary to constitute the offense intended to be punished’”).

B. Count Two Should Be Dismissed Because John Is Not a “Financial Institution” or “Money Services Business”

Count Two charges John – an individual – with the failure to maintain an effective anti-money laundering program. But such violations are appropriately charged to financial institutions and money services businesses that operate as check-cashing companies, not the individuals who own them. Since John is neither a financial institution nor a money services business, Count Two of the Indictment fails, and should be dismissed. *See United States v. Pirro*, 212 F.3d 86, 93, 95 (2d Cir. 2000) (affirming dismissal where the indictment failed to state an essential element of the crime).

The BSA requires “financial institutions” to establish AML programs. 31 U.S.C. § 5318. Pursuant to 31 U.S.C. § 5318(h)(2), the Secretary of the Treasury has prescribed minimum standards for such programs, as codified in 31 C.F.R. 1022.210(a) (which John is charged with violating). The regulation requires every “money services business” to develop, implement, and

maintain an AML program, and then provides a general framework of what is necessary for such a program. 31 C.F.R. 1022.210(b) – (d).

John is not a “financial institution,” nor has the Second Circuit held that an individual can be treated (much less criminally charged) as a financial institution for purposes of violations of §5318(h). Nor is there any Second Circuit precedent for treating a person who works for an institution that operates as a money services business, rather than the institution itself, as a “money services business.” Accordingly, Count Two clearly should be dismissed.²⁰

C. The Government’s Pre-Indictment Delay Requires Dismissal of the Indictment

Despite executing the Kayla Warrant on August 6, 2013, the Government waited almost five years to obtain an Indictment. In large part, the Indictment itself appears to be premised on information that was alleged in the Snedeker Affidavit and thus known to the Government even before it executed the Warrant. The McCue Affidavit – sworn five years later – provides no update whatsoever to what was alleged by Agent Snedeker in 2013. Patently, the five-year delay is not the product of continued investigation, but rather, is unjustifiable and unexplainable. The unwarranted delay has already prejudiced (and threatens to continue to prejudice) John, because, among other things, crucial witness testimony necessary to defend the allegations is either no longer available or may no longer be available at the time of the trial. There may be additional – and at this stage unknown – prejudice as well, because the non-specific allegations in the Indictment do not advise John which transactions he must ultimately defend, and thus do not permit the defense to marshal exculpatory testimony. Because the Government’s unnecessary

²⁰ In any event, as noted above, at all relevant times, Kayla had an AML program that satisfies 31 U.S.C. § 5318(h) and 31 C.F.R. 1022.210(a)’s mandates. As Agent Snedeker stated in his affidavit in support of the Warrant, Kayla’s AML program “includes regular and ongoing training for the employees of Kayla on current BSA laws, changes in regulations, and the employees’ responsibilities as they relate to said laws.” Siegal Aff., Ex. 1 at ¶ 28. Kayla also has a separate AML manual, a compliance officer, and outside auditors. Drago Aff. ¶¶ 2-3, *id.* Ex. 2.

and unexplained delay has compromised, and will likely continue to compromise John’s defense, the Court should dismiss the Indictment.

Generally, “a citizen’s primary guarantee against stale or long-delayed criminal prosecutions” is the statute of limitations, *see United States v. Santiago*, 987 F. Supp. 2d 465, 484 (S.D.N.Y. 2013), which “safeguards citizens from standing trial on charges whose underlying facts have grown dim with age.” *United States v. Cornielle*, 171 F.3d 748, 751 (2d Cir. 1999); *see also United States v. Marion*, 404 U.S. 307, 324 (1971) (the statute of limitations “provide[s] predictability by specifying a limit beyond which there is an irrebuttable presumption that a defendant’s right to a fair trial would be prejudiced.”). In addition to the statute of limitations, the Due Process Clause of the Fifth Amendment affords another layer of protection to defendants and safeguards against excessive and unnecessary pre-indictment delay. *See Marion*, 404 U.S. at 324; *Santiago*, 987 F. Supp. 2d at 498 (dismissing indictment on due process grounds when government brought charges 10 days before five-year statute of limitation expired); *see also Chaplin v. Kirkpatrick*, C.A. No. 9:17-CV-0718 (MAD/DEP), 2018 U.S. Dist. LEXIS 170975, at *42 (N.D.N.Y. Oct. 2, 2018) (“[D]ue process may . . . be offended even where a criminal prosecution is brought within the applicable statute of limitations . . .”).

An indictment must be dismissed where the delay (1) causes actual prejudice to a defendant; and (2) proceeding to trial would violate “fundamental conceptions of justice.” *See United States v. Gross*, 165 F. Supp. 2d 372, 377-78 (E.D.N.Y. 2001) (citing *United States v. Lovasco*, 431 U.S. 783, 790 (1977)).

A defendant suffers actual prejudice where his right to a fair trial is impaired. *See United States v. Elsberg*, 602 F.2d 1054, 1059 (2d Cir. 1979). Such deprivation may result from the loss of documentary or testimonial evidence that would have been available but for the Government’s

failure to bring the charges more promptly. *See United States v. Hillegas*, 578 F.2d 453, 460 (2d Cir. 1978); *see also Gross*, 165 F. Supp. 2d at 380-81 (finding “extreme and actual” prejudice where witnesses passed away and documents and evidence were lost); *Santiago*, 987 F. Supp. 2d at 485-86 (finding actual prejudice where government’s five-year delay resulted in the loss of exculpatory witness testimony).

In this case, because of the five-year lapse since the Government executed the Warrant, at least one critical witness, a woman in charge of filing CTRs for the 2010 to 2013 period – has retired, moved to Florida, and undoubtedly forgotten much of what she knew five or more years ago. Her testimony about how Kayla filed its CTRs and what information she was provided to file them would tend to exonerate John, but she has stated that she now barely remembers details about the general filing process, let alone specific details about transactions or customers.

Another witness – a former store manager who oversaw the day-to-day operations of the store, including when John was not in the office – is now 85 years old. Her testimony would also undoubtedly tend to exonerate John, but as more time passes, her memories will “dim.” *Marion*, 404 U.S. at 326. It bears noting that in the instant case, notwithstanding the Warrant’s execution over five years ago, nearly *nine years* have elapsed since some of the conduct is alleged to have occurred. *See* Indictment ¶ 17 (“On or about and between January 1, 2010 and October 31, 2013...”).²¹

²¹ Beyond these witnesses, the defense is not in a position at the moment to provide further details on the extent to which his ability to defend this case has been compromised due to the Government’s delay. As explained in further detail in Section VI., *infra*, at the Court’s direction, the defense repeatedly has requested a bill of particulars from the Government, and on November 21, 2018, was informed by letter that the Government would provide certain information in its Opposition to this motion. As a result, the defense remains in the dark as to the contours of the charges in the Indictment. Moreover, despite defense counsel’s repeated requests, the Government has yet to provide potentially exculpatory evidence to John, including memoranda of interviews with John’s customers. It is likely that other exculpatory testimony, like that of John’s customers, have or will become unavailable as a result of the Government’s five-year delay.

Compelling John to stand trial here in the face of the Government's delay and resulting prejudice would "violate fundamental conceptions of justice, fair play and decency," and therefore, would violate John's due process rights. *Santiago*, 987 F. Supp. 2d at 485. Indeed, an indictment should be dismissed when a defendant suffers prejudice as a result of "unjustifiable Government conduct." *See Elsberry*, 602 F.2d at 1059.

Courts within the Second Circuit have also dismissed charges when the government was grossly negligent in timely filing charges. *See, e.g., United States v. Morrison*, 518 F. Supp. 917, 919 (S.D.N.Y. 1981) (dismissing indictment for pre-indictment delay based on finding that government's gross negligence deprived the defendant of the opportunity to interview and present witnesses who had exculpatory testimony); *Schurman v. Leonardo*, 768 F. Supp. 993, 998 (S.D.N.Y. 1991) (noting that "reckless disregard of the circumstances" by the government could result in dismissal of indictment).

Here, the Government does not offer any justification for its delay. It appears that the Government's investigation hit a standstill at some point shortly after it executed the Warrant, and was not revisited until a few years thereafter for unknown reasons. Nothing, however, suggests that the delay was attributable to active pursuit of an ongoing investigation. The Indictment's allegations largely track what was included in the Snedeker Affidavit, which was drafted before the Warrant was executed.

As a result of the Government's inexplicable delay, John's ability to defend himself has been irreparably prejudiced. *See United States v. Jackson*, 488 F. Supp. 2d 866, 873 (D. Neb. 2007) (dismissing indictment where case file "languished on the desk [of the prosecutor] for two years" because "[t]here was an intentional decision not to make this a priority case..."); *cf. Symonds v. Griffin*, No. 15 CV 9423 (PGG) (KNF), 2018 U.S. Dist. LEXIS 105079, at *14

(S.D.N.Y. June 21, 2018) (emphasis added) (stating that “no evidence exists that anyone delayed the prosecution intentionally in order to gain a tactical advantage *or simply neglected the case for no reason*”).

Under the present circumstances, requiring John to face trial in the face of the Government’s inexplicable delay would offend traditional notions of justice and fair play. *Lovasco*, 431 U.S. at 790. In the interests of justice, the Indictment should be dismissed.²² Alternatively, John reserves the right to supplement this motion at a later date in the event and to the extent that further elements of prejudice become clear from any later production of discovery and/or materials produced pursuant to *Brady* and *Giglio*.

VI.

THE GOVERNMENT SHOULD PROVIDE A BILL OF PARTICULARS

For the reasons discussed above and more specifically below, this Indictment fails adequately to put John on notice of the charges against him sufficient for him to mount his defense. Here, the indictment lacks sufficient detail in three overarching respects, among others: (1) Count One of the Indictment fails to inform John when and under what circumstances – over *more than three- year period*, he willfully failed to file one or more CTRs (especially given that he filed more than 8,000 CTRs in that time frame); (2) similarly, Count Three of the Indictment fails to inform John when and under what circumstances – over a similarly lengthy span – he intentionally structured one or more transactions to avoid filing CTRs, and (3) Counts Four through Eight fail to inform John when, and with respect to which employees, John intentionally

²² Alternatively, a hearing should be held to determine the reasons for the Government’s delay in indicting John and whether the delay was justified. *See United States v. Wai Ho Tsang*, 632 F. Supp. 1336, 1339 (granting request for evidentiary hearing to determine reason for pre-indictment delay); *see also Gross*, 165 F. Supp. 2d at 380 (conducting fact-based inquiry and rejecting government’s attempt to categorize delay as “investigative delay” where in the six years since the start of the investigation, the government’s failure to act was evidenced by large gaps of time with no case activity).

failed to collect and pay FICA taxes, and in what amounts. Accordingly, the Court should order the Government to provide the defense with a bill of particulars, supplying the missing, basic information necessary to elucidate the charges.²³

The Sixth Amendment affords every criminal defendant the right “to be informed of the nature and cause of the accusation.” U.S. Const. Amend. VI. Therefore, the Government is required to provide a bill of particulars where “the charges of the indictment are so general [] they do not advise the defendant of the specific acts of which he is accused.” *See Scully*, 108 F. Supp. at 125; *see also* Fed. R. Crim. P. 7(f). This is certainly the case here.

As the Second Circuit has explained, a defendant may seek a bill of particulars to obtain “information about the details of the charge against him if this is necessary to the preparation of his defense, and to avoid prejudicial surprise at trial.” *See United States v. Bortnovsky*, 820 F.2d 572, 573-74 (2d. Cir. 1987) (holding that the district court abused its discretion in denying defendant’s motion for a bill of particulars seeking to identify the false statements in more than 4,000 pages of insurance claims); *see also United States v. Zhong*, No. 16-cr-614 (DLI), 2017 U.S. Dist. LEXIS 175357, at *6 (E.D.N.Y. Oct. 23, 2017) (granting request for bill of particulars to identify false statements in visa applications because “preparing a defense for every statement” would “impermissibly . . . shift the burden of proof to Defendant.”).

A. The Ambiguity of the Indictment Warrants a Bill of Particulars

A bill of particulars is warranted where, as here, “the charges of the indictment are so general that they do not advise [John] of the specific acts of which he is accused.” *United States v. Nekritin*, 10-cr-491 (S-1) (KAM), 2011 U.S. Dist. LEXIS 47407, at *20, *26 (E.D.N.Y. May

²³ As per the Court’s instructions at the September 25, 2018 pre-trial conference, defense counsel has requested from the Government a bill of particulars. Indeed, the defense provided the Government in writing with an itemized list of the particulars sought with respect to each of the counts in the Indictment. The Government has declined to provide particulars, instead insisting that we move the Court for this relief. Siegal Aff. ¶ 18.

3, 2011) (granting request for bill of particulars where otherwise the defendants “are left to determine which claims for which beneficiaries are alleged to form the basis of the . . .fraud” and defendants would be forced “to defend legitimate claims unrelated to the ... charge.”); *United States v. Stern*, No. 03 Cr. 81 (MBM), 2003 U.S. Dist. LEXIS 20936, at *11 (requiring government to specify “wrongful conduct that [defendant] was allegedly seeking to conceal” because “he should not be forced to speculate what the government may have some other wrongful act in mind that it intends to spring upon him at trial”); *United States v. Bin Laden*, 92 F. Supp. 2d 225, 235 (S.D.N.Y. 2000) (requiring bill of particulars where “the allegations contained in the ‘Overt Acts’ section of the Indictment are cast in terms that are too general ... to permit Defendants to conduct a meaningfully directed investigation of the relevant facts and circumstances and be prepared to respond to the charges.”)

The Indictment charges John with eight different counts and spans a mere 10 pages, though more than half the language amounts to general charging language. The Indictment fails to: specify any transactions, explain any wrongdoing, or mention any people (other than John). Given the complete absence of any detail here, “the potential for unfair surprise and the difficulty of preparing a defense are amplified.” *See Rajaratnam*, 02010 U.S. Dist. LEXIS 70385, at *4. In light of the nature of the charges against John, such vagueness leaves him to guess which “one (or more)” transactions for a more than three-year period the Government intends to prosecute, or which one of his more than 25 employees he is alleged to have failed to collect pay taxes for at some point in one of five different tax reporting periods.

For example, Count One charges John with causing and attempting to cause Kayla “to fail to file one or more” CTRs as “part of a pattern of illegal activity involving more than \$100,000 in a 12-month period” at some point between January 1, 2010 and October 31, 2013.

The count does not specify the date of the alleged transactions, the customer names, transaction amounts, or transaction locations for any alleged failure to file – in other words, anything that would allow John to ascertain which CTR (or which CTRs) he is alleged to have failed to file.

See Indictment ¶¶ 1-17. As the Indictment stands now, the defense cannot determine which “one or more” – in the roughly half a million – check-cashing transactions that took place during this time frame are at issue, nor for which of Kayla’s nearly 10,000 customers CTRs should have been filed.

Similarly, Count Three charges John with structuring or assisting in structuring “one or more financial transactions” between August 1, 2010 and October 1, 2013. As with Count One, Count Three does not specify the date of the alleged structuring, the transactions alleged to have been structured, or the identities of the customers at issue. *See Indictment ¶¶ 1-15, 22-23.*

Again, the defense is left to guess which “one or more” individual transactions among literally of *hundreds of thousands* conducted by the business in that time span, was/were structured to avoid triggering CTR filing.

Indeed, the lack of specifics in Count Three prevents the defense from ascertaining whether this Count is duplicitous (which it very well may be). (*See supra*, Section V.A.). If the Government seeks to prosecute John for more than one instance of structuring – and Count Three does not specify even that much –then Count Three would be duplicitous for the same reasons that Count One is. Without more information, it is impossible for the defense or the Court to address the issue of whether Count Three should also be dismissed as constitutionally infirm.

Given the sheer number of potentially relevant transactions at issue, the defense cannot effectively review hundreds of thousands of individual transactions to find the “one or more” that the Government purports were criminal, without a more particularized understanding of the

Government's charges. As explained above, Kayla has engaged in hundreds of thousands of transactions for thousands of customers during the time periods that the Government alleges in the Indictment, and has filed more than 8,000 CTRs in the relevant time period. At this stage, the defense can only speculate as to which of these transactions could be the subject of the Government's structuring allegations.

Count Two's allegations that John failed to maintain an effective AML program appear to be based on the allegations of Counts One and Three. To the extent that Count Two is premised on Kayla's purported failure (despite having an AML program) to prevent the alleged non-filing of required CTRs and to prevent the alleged structuring, the lack of detail in Counts One and Three also render Count Two improperly lacking in particulars. Count Two does not provide details on when CTRs were not filed, when John allegedly agreed to accommodate customers' requests not to file CTRs (or for which customers), or when he failed to provide accurate records of customers' cash transactions so that Kayla's employees could file CTRs (or for which customers).

John and counsel are effectively left to mine through a list of hundreds of thousands of transactions and wager a "best guess" as to what the Government is alleging, impermissibly shifting the burden to John to prove a negative. *United States v. Trie*, 21 F. Supp. 2d 7, 21 (D.D.C. 1998) ("Not only does the government's position presume that the defendant knows what the government alleges that he did and with whom he dealt and therefore has all the information he needs, a premise inconsistent with the presumption of innocence, but it smacks of gamesmanship."); *see also United States v. Savin*, No. 00 Cr. 45 (RWS), 2001 U.S. Dist. LEXIS 2445, at *10 (S.D.N.Y. Mar. 13, 2001) (ordering bill of particulars where the indictment alleged that defendant pilfered his client's money through unspecified intercompany transfers without

identifying the amounts, dates, means, corporate entities, or co-conspirators involved). “The fact that a defendant may have some, or even all the information requested, does not necessarily defeat his right to a bill of particulars . . . a defendant is presumed to be innocent and hence, [] it must be assumed he is ignorant of the facts on which the pleader founds his charges.” *United States v. Spur Knitting Mills, Inc.*, 187 F. Supp. 653, 654 (S.D.N.Y. 1960) (granting bill of particulars and holding that the defendant “is entitled to this information in order properly to prepare to meet the charges and to avoid surprise upon the trial.”).

Courts in this very District have granted requests for a bill of particulars when numerous transactions could potentially be at issue, but are not detailed in an indictment. *See, e.g., United States v. Hawit*, No. 15-cr-252 (PKC), 2017 U.S. Dist. LEXIS 23391, at *30 (E.D.N.Y. Feb. 17, 2017) (“Without a detailed list of those allegedly tainted transactions, [defendant] and his counsel will be in the same position as the criminal defendants who were deemed entitled to bills of particulars in [other cases]: accused of having committed unlawful acts in connection with a category of transactions, but without being given notice of which specific transactions falling within that category are alleged to have been tainted by unlawful conduct.”); *United States v. Onassis*, 125 F. Supp. 190, 213-14 (D.D.C. 1954) (ordering bill of particulars for, among other items, “the names of all persons and the dates of all transactions [the government] will rely upon as involved...” in a conspiracy to falsify applications before a government agency); *see also United States v. Luna*, No. 3:05cr58 (SRU), 1006 U.S. Dist. LEXIS 28947, at *4 (granting bill of particulars for the list of transactions in which the defendant was allegedly involved, including the names of the other parties involved, the nature and the amount of the drug, and the approximate date and location of such transactions); *United States v. Raue*, CR 07-31000-02, 2008 U.S. Dist. LEXIS 91827, at *11 (D.S.D. Nov. 12, 2008) (requiring government to provide

the approximate date and time of day when defendant was alleged to receive a bribe, the person who allegedly bribed the defendant, the place of bribery, and the form of payment).²⁴

Counts Four through Eight are similarly devoid of information. The Government alleges that at some point between April 1, 2012 and July 31, 2013, John failed to collect and remit FICA taxes to the IRS. These Counts do no more than list the due dates for tax forms. The Indictment does not name the employees for whom taxes were not collected, when the taxes were allegedly not collected, nor the amount of taxes that were allegedly not collected. Nor does the discovery provided to date support the charges, because the Government has produced Hogwart's annual corporate tax returns (Forms 1120) and its quarterly federal tax returns (Forms 941). Nowhere on these forms is there an employee's name, nor any other information that would inform the defense as to when John is alleged to have underreported a given employee's gross wages, which employee was paid off the books, or how much tax Kayla owed. As with Counts One and Three, the defense can only guess as to what John is alleged to have done wrong.

Given the complexity of criminal tax cases in particular and various methods of proof, requests for bills of particulars are "quite freely granted" in such cases. *See United States v. O'Connor*, 237 F.2d 466, 476 n.10 (2d Cir. 1956); *United States v. DeGroote*, 122 F.R.D. 131,

²⁴ Courts have repeatedly held that indictments that already include the information being requested here are sufficient to apprise the defendant of the claims against which he must defend. *See, e.g., United States v. Gasperini*, No. 16-CR-441 (NGG), 2017 U.S. Dist. LEXIS 84116, at *29-30 (E.D.N.Y. May 31, 2017) (finding that the risk of unfair surprise is obviated when the defendant is told which transactions were alleged to constitute money laundering and what the alleged purpose of the transactions at issue were); *United States v. Walters*, 963 F. Supp. 2d 125, 134 (E.D.N.Y. 2013) (noting that an indictment that "provides information as to the nature of the allegedly fraudulent scheme, its timing and its participants, and the specific ... transfers giving rise to the ... charges" is "sufficient"); *United States v. Leon*, No. 1:08-CR-65-1, 2008 U.S. Dist. LEXIS 93751, at *3 (D. Vt. Nov. 18, 2008) (holding that the Government's provision of the "date of each money laundering transaction, as well as [many] cash receipts" provided defendant with "sufficient notice to prepare a defense"); *United States v. Belkin*, No. 93-240, 1993 U.S. Dist. LEXIS 17202, at *17 (E.D. Pa. Dec. 8, 1993) (finding a count which specified the "deposit dates and the amounts of the checks that are the subject of" the counts to contain "sufficient details").

141 (W.D.N.Y. 1988) (noting that the Second Circuit has “disapproved” of restrictive approaches to requests for bills of particulars in the tax context). As in *DeGroote*, where the Government did not specify the amounts of unreported or underreported income at issue, “[t]he requirement of particulars . . . serves the salutary purpose of identifying for the defendant the blocks of alleged income to which the indictment is directed and to which a defense must be prepared.” *DeGroote*, 122 F.R.D. at 142; *see also United States v. Deluca*, No. 11-CR-169A(F), 2013 U.S. Dist. LEXIS 145364, at *9-11 (W.D.N.Y. Oct. 7, 2011) (ordering Government to provide precise dates, characters, and amounts of unreported income where previously provided bill of particulars provided information that was “included but not limited to” the listed particulars and thus left the scope of the Government’s case virtually open ended).

John is not making some idle request, nor is he requesting information that he has received in an acceptable alternative format, nor is he asking the Government to detail exactly how it plans to prove its case. *See Scully*, 108 F. Supp. 3d at 59. Rather, he is asking to be apprised of what he is accused of doing wrong in a way that is marginally more specific than simply citing to the statute he is charged with violating. Without this information, John will be forced to unnecessarily waste time and resources poking blindly through discovery (much of which has not yet been provided) trying to figure out what the Government is alleging, despite the Government’s obligation to provide John with an adequate Indictment that gives the essential facts constituting the offense charged. *See Fed. R. Crim. P. 7; Trie*, 21 F. Supp. 2d at 21 (“A defendant . . . should not have to waste precious pre-trial preparation time guessing which statements he has to defend against or which contributors may be witnesses against him at trial when the government knows precisely the statements on which it intends to rely and can easily provide the information.”)

B. John's Request Is Narrowly Tailored to Seek Only that Information Necessary to Prepare His Defense and Avoid Unfair Surprise at Trial

John's request is narrowly tailored to seek discrete categories of information that are necessary in the preparation of his defense to these charges, and to avoid unfair surprise at trial. John can only prepare to defend the Government's charges for failing to file one or more CTRs, for structuring, and for failing to have an effective AML program (based on the CTR and structuring charges) if he is apprised of the transactions and customers at issue. *See Savin*, 2001 U.S. Dist. LEXIS 2445, at *10 (granting request for particulars where defendant would otherwise be forced to "comb through" thousands of pages of documents to "attempt to guess at" which transactions were allegedly improper); *Bortnovsky*, 820 F.2d at 574 (defendant entitled to know dates of staged burglaries and identity of fraudulent documents to prepare for trial and not be subject to surprise). Similarly, he can prepare to defend himself against the Government's tax-related offenses only if he is apprised of the employees for whom taxes were not collected, when the taxes were allegedly not collected, and amounts of tax at issue. *See DeGroote*, 122 F.R.D. at 142 ("The requirement of particulars, particularly as to approximate amounts of unreported or underreported income, serves the salutary purpose of identifying for the defendant the blocks of alleged income to which the indictment is directed and to which a defense must be prepared.")

The Indictment also presents the vague allegation that John "caused" Kayla to fail to file one or more CTRs. John can only defend against these allegations if he is on notice of how he allegedly "caused" Kayla (or its employees) to act and who those employees may be. *See United States v. Hsia*, 24 F. Supp. 2d 14, 32 (D.D.C. 1998) ("[T]he government still has not provided a coherent explanation of how Ms. Hsia 'caused' those false statements to be made. Accordingly, the Court will order a bill of particulars disclosing how Ms. Hsia is alleged to have caused each

of the false statements to be made); *see also Trie*, 21 F. Supp. 2d at 22 (stating that the Government must provide details of how defendant “caused [false statements] to be made”).

Accordingly, the Government should be required to specify the missing particulars so that John can adequately prepare for trial. The Court should order the Government to provide the following particulars:

1. Information sufficient to identify each alleged transaction for which John failed to file a required CTR, including but not limited to at least:
 - a. the dates on which these transactions and alleged failures occurred
 - b. which customers were involved with the transactions
 - c. the amount at issue in the transactions that allegedly required a CTR to be filed
 - d. the location(s) where these alleged failures occurred
2. Information sufficient to identify each act that allegedly contributed to the charge that John failed to maintain an effective anti-money laundering program:
 - a. the dates on which these allegedly problematic transactions occurred
 - b. the manner in which John is alleged to have prevented the implementation and maintenance of an effective anti-money laundering program
 - c. which customers were involved with the transactions and for whom John allegedly agreed to accommodate requests that CTRs not be filed
 - d. the amount at issue in the transactions
 - e. the location(s) where these alleged transactions occurred
3. Information sufficient to identify each allegedly structured transaction, including but not limited to at least:
 - a. the dates on which these transactions and alleged structuring occurred
 - b. which customers were involved with the transactions
 - c. the amount at issue in the transactions that allegedly required a CTR to be filed
 - d. the location(s) where these alleged failures occurred
4. Information sufficient to identify the employees and tax quarters for which John allegedly failed to collect and pay FICA taxes, including but not limited to at least:
 - a. the names of the employees for whom John allegedly failed to collect FICA taxes
 - b. the months when John allegedly failed to collect FICA taxes
 - c. the amount of tax alleged to be at issue
5. Information sufficient to put the defense on notice of how John allegedly “caused” Kayla to fail to file CTRs.

6. Information sufficient to put the defense on notice of how John allegedly “caused” Kayla to structure transactions.

VII.

THE GOVERNMENT SHOULD BE ORDERED TO PRODUCE BRADY AND GIGLIO MATERIAL

The Government should immediately produce all *Brady* and *Giglio* material. In particular, the Government should produce specific material the defense has identified and expressly requested – namely, interviews of customers and/or present or former employees whose statements would tend to undermine, contradict or refute the Indictment’s allegations. “Under *Brady* and its progeny, ‘the Government has a constitutional duty to disclose favorable evidence to the accused where such evidence is ‘material either to guilt or to punishment.’’’ See *United States v. Brown*, 10-CR-675 (SJF), 2011 U.S. Dist. LEXIS 81595 at *18-19 (E.D.N.Y. July 25, 2011) (Feuerstein, J.) (quoting *United States v. Paulino*, 445 F.3d 211, 224 (2d Cir. 2006); see also *United States v. Rodriguez*, 496 F.3d 211, 225 (2d Cir. 2007) (Government required to disclose material that is favorable “either because it is exculpatory, or because it is impeaching”). Such disclosure “recognizes the possibility that the evidence on which the prosecution relies to prove the defendant’s guilt is not necessarily truthful, accurate, or complete,” especially where the prosecution is aware of evidence that is favorable to the defense. *Rodriguez*, 496 F. Supp.3drnment must produce *Brady* material “in time for its effective use” so as to not deprive a defendant of his due process rights. See, e.g., *United States v. Coppa*, 267 F.3d 132, 144 (2d Cir. 2001) 113; *United States v. Taylor*, 17 F. Supp. 3d 162, 177 (E.D.N.Y. 2014) (same). This Court may order *Brady* and *Giglio* disclosures at any time as a matter of “sound case management.” See *Taylor*, 17 F. Supp. 3d at 177; cf. *United States v. Mahaffy*, 693 F.3d 113, 133 (2d Cir. 2012) (stating that the government’s *Brady* violations negatively impacted

case because the trials “were both unfairly skewed” and “the costs of this litigation – in terms of personal, financial and judicial resources and time – have ballooned...”).

The defense requested *Brady* and *Giglio* materials on September 25, 2018, and later, in writing by letters and emails dated October 8, 2018, October 23, 2018, and November 7, 2018. *See Siegal Aff.* ¶¶ 13-16; Ex. 9-11. Among the items that counsel has already requested, but that the Government has not produced, are any memoranda, notes or minutes from interviews of John’s customers, employees, or former employees to the extent those materials discuss John or Kayla. The defense believes that one or more such interviewed individuals would have and did report to the Government that John was very attentive to BSA and AML requirements, and that he played by the rules. To the extent the Government received such, it must review and produce any notes and memoranda prepared by its agents, including other AUSAs and IRS agents, reflecting such information. *See, e.g., United States v. Triumph Capital Grp., Inc.*, 544 F.3d 149, 61-62 (2d Cir. 2008) (overturning conviction where Government failed to disclose interview notes taken by FBI that contained *Brady* material); *United States v. Gupta*, 848 F. Supp. 2d 491, 495-96 (S.D.N.Y. 2012) (stating that where there is investigation involving more than one agency, “*Brady* ... requires more than assuming no new exculpatory information will be found. There is no transcript that serves as a complete and accurate record of what was said at these interviews. The SEC attorney may have chosen to emphasize other parts of the witness interviews in his memoranda that did not make it into the FBI’s agent’s notes, or that the Government attorneys present simply forgot, and those may qualify as *Brady* material.”). Accordingly, the Government should immediately produce *Brady* and *Giglio* material.

CONCLUSION

For all these reasons, John respectfully requests an Order (1) suppressing the evidence and fruits of the 2013 search of Kayla; (2) suppressing the evidence and fruits obtained from his

cell phone; (3) dismissing the Indictment (or certain Counts); and (4) requiring the Government to provide a bill of particulars and *Brady* and *Giglio* materials.

Dated: November 30, 2018

MINTZ LEVIN COHN FERRIS
GLOVSKY AND POPEO, P.C.

By: /s/ David M. Siegal
David M. Siegal
Jason P.W. Halperin
Amanda B. Asaro
Chrysler Center
666 Third Avenue, 25th Floor
New York, New York 10017
(212) 935-3000